OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

CROSS-SECTOR

14 February 2020 **LIR 200214003**

Online Doxing and In-Person Harassment of Private Sector and United States Government Individuals

FBI Houston, in coordination with InfraGard, Houston Police Department, Houston Regional Intelligence Service Center, and the FBI's Office of Private Sector (OPS), prepared this LIR to inform private sector and law enforcement partners of in-person and online doxing[a], potentially putting private sector, local, state and federal government individuals at risk of cyber-stalking. Victims of the online doxing are located in cities and states such as Houston, Texas, Los Angeles, California, New York, New York, Washington, DC, Boston, Massachusetts, Arizona, Colorado, and Florida. An online website is calling for its members to begin doxing more victims in other cities and states. The online doxing is publically posted and includes personal information such as residential address, telephone and email, property value, and employer information associated with board members in the private sector, as well as state, local, and federal officials.

In one city, in-person harassment included hand delivered cease and desist letters[b] to victims' (e.g. private sector stakeholders associated with InfraGard, Office of Emergency Management personnel, and federal government executives), residential address and place of employment as well as fliers[c] distributed to neighbors accusing the victim of involvement in "gangstalking."

According to the website, "gangstalking" is the practice of attacking civilians with psychological torture techniques, including stalking, harassment, and intimidation." The website identifies personally identifiable information (PII) through publicly available sources, such as county housing appraisal and tax records, veripages.com, and zabasearch.com. Based on a review of statements made on the website, the site lists over 100 "targeted individual" websites in the United States and foreign countries. The actor's activity includes mining the Internet for PII from social media platforms, public databases for addresses, and websites which contain resumes. The actors used the information to conduct online doxing against individuals associated with the FBI, DHS Fusion Centers, and InfraGard; however, in one city targeted by the actors, the activity was followed by in-person, physical targeting and harassment of public-private individuals.

Protecting Your PII in the Digital Age

The FBI suggests use of good cyber hygiene, such as reputable antivirus, malware software, firewall, and personal computer use practices to include:

- Be aware of public records, such as tax and housing appraisal records

[a] Doxing is a common practice among hackers in which a hacker publicly releases identifying information of a victim including full name, date of birth, address and pictures. Information used in doxing may be obtained from filtrated data, or doxing can occur by collecting and assembling accessible information and disseminating it to the public.

[b] See Appendix A: Copy of Cease and Desist Letter Delivered to Private Residences

[c] See Appendix B: Copy of Flier Delivered to Private Residences and Neighbors of Victims

- Remove your name from people search lists and personal information about you or family members
- Create multiple usernames and email addresses
- Change passwords often and use strong passwords mixing letters, numbers, and symbols; do not reuse passwords for multiple accounts
- Monitor online personal information, including what others post about you on social networking sites
- Be aware of data sharing and sites that sell your personal information
- Monitor credit reports
- Use multi-factor authentication
- Be careful when giving out personal contact information and do not reuse passwords for multiple accounts
- Increase social network privacy settings, such as disable public visibility of your social media accounts

Indicators of online doxers identified as "targeted individuals[d]" threatening their victims include and are not limited to the documented activities listed below.

- Disseminating fliers and/or a cease and desist letter accusing them of "attacking civilians with psychological torture techniques," taped to the door of their private residence, and posted online

- Hand-delivering to neighboring residences conspiracy letters stating their neighbors were federal government employees, alleging involvement in criminal activity, questioning how federal government personnel could afford their homes on government salaries and listing their address and open source tax appraisal value of their home

- Hand delivering letters to their victims residential mailbox

- Delivering package(s) addressed to victim(s) at their place of employment with a return address to "TargetedJustice"

- Disseminating doxing email(s) entitled "Cease & Desist letter," alleging the identified executives were engaging in "gangstalking," and/or an email "demand[ing] an explanation for these activities and compensation for pain, suffering, and illegal torture"

[d] Targeted Individuals are a group of people that organize around the conviction they are victims of a sprawling conspiracy to conduct continuous physical and electronic surveillance, illegally harass them with torture, mind-controlled weapons and a low frequency of electromagnetic waves, causing them to experience psychotic symptoms. They allege they are being "gangstalked" by several entities to include the government, financial elite, aliens, their neighbors, freemasons or a combination of any of these groups.

Hearing the following key words or phrases suggest you are likely dealing with a person who self identifies as a doxer /"targeted individual" If you encounter such an individual, and you feel threatened call 911.

- "Target Justice"
- "Targeted Individual"
- "TI"
- "GangStalking"
- "Organized Gangstalking,"
- "Voice-to-skull technology" (V2K)
- "Directed-Energy Weapons" (DEW)
- References to Racketeering Influenced and Corrupt Organizations (RICO), the Geneva Convention and human trafficking

If any fliers or packages containing a cease and desist letter are received by email, mail and/or in-person delivery, report the activity to your local security office, local law enforcement and/or the FBI. Suspicious emails can be reported to www.IC3.gov.

This LIR was disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices.

xpand Download

Appendix A: Copy of Cease and Desist Letter Delivered to Female Residence

[redacted]

It is my opinion, that you and your organization are involved in a serious crime, called gangstalking. I have compelling records and evidence that you are attacking civilians with psychological warfare technologies, including stalking, gangstalking, harassment, and intimidation.

I am part of a larger group representing the interests of more than 2,500 Targeted Individuals ("Non-Investigative Subjects"). We demand an explanation for these activities and compensation for pain, suffering, and illegal actions. A similar letter has been sent to General John Raymond at the Air Force Space Command, where he is involved with illegal satellite tracking and microwave weapons.

We have sworn affidavits from 2 FBI agents, confirming that this illegal program is occurring. We have the training manual for gangstalking, and we have the FBI's secret manual, covering these covert operations. We have statements from 25 Medical Doctors confirming that this program exists.

You can be sued in a Civil Court for your criminal activity.

I demand that you immediately CEASE AND DESIST your illegal activities, including the use of government personnel and external groups, such as Infragard and Citizen Corps, which may also be participating. Such operations are in violation of Article 52 of the Geneva Conventions (psychological torture) and numerous Federal & State laws.

This CEASE AND DESIST ORDER is to inform you that your harassing, stalking, and intimidation actions are illegal and will not be tolerated. I demand that you immediately CEASE AND DESIST. Should you continue to pursue these activities in violation of this CEASE AND DESIST ORDER, I will not hesitate to pursue legal action against you.

This CEASE AND DESIST ORDER demands that you immediately discontinue and do not at any point in the future, under any circumstances, do the following: pursue, harass, attack, strike, bump into, brush up against, push, tap, grab, hold, threaten, telephone (via cellular or landline), instant message, page, fax, email, follow, track, shadow, disturb the peace, keep under surveillance, hack electronic devices, gather information about and/or block movements at home, work, social gatherings, in public areas, or religious functions.

You may have already violated numerous Federal & State laws, including:

- 18 U.S. Code § 2381, Treason
- 18 U.S. Code § 2340, (a) Conspiracy to commit torture.
- 18 U.S. Code § 2382, Misprision of Treason.
- 18 U.S. Code § 2384, Seditious Conspiracy.
- 18 U.S. Code § 2385, Advocating for actions against the United States.
- 18 U.S. Code § 241, Conspiracy to Deprive Constitutional Rights.
- 18 U.S. Code § 242, Deprivation of Constitutional Rights.
- 18 U.S.C. § 2261A Interstate Stalking.
- 18 U.S.C. § 875(c) Interstate communications.
- 47 U.S.C. § 223(a)(1)(C) Harassing Telephone Calls.
- 18 U.S. Code § 2421, Organized Crime Control Act of 1970 (OCCA).
- [redacted]

Should you choose to continue your actions and attacks, I will not hesitate to file complaints and publicly expose your ongoing criminal activity.

[redacted]