Mitigating the Impacts of Doxing on Critical Infrastructure

May 12, 2021

WHAT IS DOXING?

Doxing refers to the internet-based practice of gathering an individual's personally identifiable information (PII)—or an organization's sensitive information— from open source or compromised material and publishing it online for malicious purposes. Although doxing can be carried out by anyone with the ability to query and combine publicly available information, it is often attributed to state actors, hacktivists, and extremists.

Doxers compile sensitive information from compromises of personal and professional accounts and a wide range of publicly available data sources to craft invasive profiles of targets, which are then published online with the intent to harm, harass, or intimidate victims.

EXAMPLES OF SENSITIVE INFORMATION

- Full Name
- Contact Information
- Home Address
- Family Members
- Workplace Details
- Financial Information
- Social Security Number

COMMON SOURCES OF INFORMATION

- Social Media Posts
- Property and Court Records
- Wedding Announcements and Obituaries
- Newsletters
- Public Conferences
- Web Forums, Blogs, and Discussion Boards
- Unprotected networks
- Voter Registration Lists

POTENTIAL IMPACT TO CRITICAL INFRASTRUCTURE

Like many other businesses, critical infrastructure organizations maintain digital databases of PII and organizationally sensitive information, making them ripe targets for doxing attacks. Threat actors may target critical infrastructure organizations and personnel with doxing attacks as a result of grievances related to organizational activities or policies. Incidents of doxing that target personnel and facilities often serve to harass, intimidate, or inflict financial damages, and can potentially escalate to physical violence.

Doxing also poses a threat to senior leadership of critical infrastructure organizations, who may be targeted due to their elevated position with the organization or stance on a particular issue. Doxing attacks targeting senior leaders often serve as "reputation attacks" and could lead to activities seeking to embarrass, harass, or undermine confidence in an official.

CASE STUDIES

There are several notable doxing incidents targeting critical infrastructure sectors that underscore the threats posed to individuals and organizations:

2014

A hospital was targeted by hacker group Anonymous for its handling of a high-profile child custody case. The first stage of the cyberattack involved threats on social media containing personal information, home and work addresses, email addresses, and phone numbers of some of the individuals involved in the case. Shortly following the threatening posts, Anonymous executed a distributed denial-of-service (DDoS) attack that compromised hospital systems.

2016

Protest activity surrounding an underground oil pipeline resulted in the targeting of law enforcement officers responsible for securing the pipeline and protests. Protestors used nametags worn by law enforcement to identify, research, and share personal information about officers online—including pictures, dates of birth, and addresses. Online posts called for attacks on law enforcement and their families, resulting in some being followed or reporting suspicious vehicles parked outside of their houses.

2020

After the 2020 U.S. Presidential Election, high-profile individuals were targeted as a result of their affiliations or stance on the election. CISA and the FBI reported that Iranian actors created a website that published sensitive personal details of governors, secretaries of state and other elections officials, and people working for election technology companies. A senior employee of a voting machine company had personal information and the addresses of family members and romantic partners posted online, resulting in some receiving threatening letters and the employee going into hiding after receiving death threats.

PROTECTIVE & PREVENTATIVE OPTIONS FOR INDIVIDUALS AND ORGANIZATIONS

To mitigate the effects of doxing, individuals and organizations can protect themselves by taking an active role in controlling the information that is shared and stored online and implementing a series of best practices.

Social Media

Social networking sites provide a wealth of information that can be used by doxers. Consider conducting an audit of both personal and organizational social media accounts and implementing several changes.

- Check security and privacy settings and implement the strongest controls possible.
- Deactivate or delete any profiles no longer in use.
- Review followers and unfollow or reject requests from anyone unknown.
- Remove any PII (address, date of birth, phone number, etc.) from social media profiles.

Spear Phishing and Social Engineering

Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information.

Software Updates

Cybercriminals are always looking for ways to install malware that captures personal data, payment information, and passwords. Update all software, operating systems, and applications to the most recent versions, and only apply updates from a trusted source.

Removed Unwanted Apps and Extensions

Mobile apps and browser extensions, such as downloadable in-browser tools that block ads, are known to collect personal data. This data collection often occurs without the full knowledge or consent of the user. Review apps and browser extensions frequently and remove any that are unnecessary or not in use.

Conduct frequent internet searches for unwanted pictures and information that may be found online. Assume that anyone can see personal information that is shared online.

Public Records Websites

Public records websites periodically scrape public-facing websites and compile information that may include names of relatives, addresses, photographs, real estate records, and more. Regularly request that personal information be removed from these sites.

MITIGATION OPTIONS: WHAT IF YOU BECOME A VICTIM?

After taking the necessary proactive steps to secure and limit personal information online, personnel and their families still may be at risk. If a compromise and release of personal or sensitive information occurs, consider these steps:

Report the Incident
Report the incident to your organization's security office, local law enforcement agency, social media platform, and website administrators. Document what occurred and take screen shots to share with investigators and administrators. Consider reporting the incident to the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3).

Understand the Threat
Determine what information was exploited, the seriousness of the threat, and the point of compromise.

Remove the Information
Work with website administrators and cybersecurity professionals to remove information from websites or applications. Configure privacy settings to the most private options.

Monitor Safety
Watch for signs of identity theft, monitor financial accounts, set up fraud alerts, and change log-in and password information for all online accounts. If concerned about physical safety, contact local law enforcement for next steps.

ADDITIONAL RESOURCES & GUIDANCE

CISA Cybersecurity Best Practices & Resources: cisa.gov/cybersecurity

CISA Cyber Essentials: cisa.gov/cyber-essentials

CISA Cybersecurity and Physical Security Convergence Guide: cisa.gov/cybersecurity-and-physical-security-convergence

CISA Insights: Enhance Email and Web Security: cisa.gov/publication/enhance-email-and-web-security

CISA Tip: Securing Network Infrastructure Devices: cisa.gov/tips/st18-001

CISA Tip: Preventing and Responding to Identity Theft: cisa.gov/tips/st05-019

CISA Tip: Avoiding Social Engineering and Phishing Attacks: cisa.gov/tips/st04-014

CISA Tip: Guidelines for Publishing Information Online: cisa.gov/tips/st05-013

CISA Protective Security Advisors: cisa.gov/protective-security-advisors

Elections Infrastructure Information Sharing and Analysis Center (ES-ISAC) Cybersecurity Spotlight - Doxing: cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-doxing/

Multi-State Information Sharing and Analysis Center (MS-ISAC) Security Primer - Securing Personal Social Media Accounts: cisecurity.org/white-papers/cis-primer-securing-personal-social-media-accounts/

If you are a victim of online crime, file a complaint **with the FBI's Internet Crime Complaint Center (IC3**) at ic3.gov.

National Capital Region Threat Intelligence Consortium/New York State Intelligence Center - Doxing Mitigation Guide: rit.edu/security/sites/rit.edu.security/files/Cyber_Advisory-DoxingMitigation-TLPWHITE_1.pdf

For more information or to seek additional help, contact us at Central@cisa.gov.