Navigare nel Mare dei Dati Hackerati

Redazione | 28/04/2025 | Sicurezza digitale

Dati Hackerati | Una Guida Pratica per il Giornalismo Investigativo

Negli ultimi anni, il panorama del giornalismo investigativo ha subito una trasformazione radicale. La sfida principale non è più ottenere informazioni, ma **dare un senso alla quantità enorme di dati disponibili**, spesso rilasciati da hacker e whistleblower. Questi "tesori" digitali, provenienti da governi, aziende e intermediari finanziari, possono essere miniere d'oro di informazioni di interesse pubblico, ma presentano anche **nuove sfide etiche, legali e logistiche**. Ecco una guida pratica per navigare in questo complesso scenario.

Dove Trovare i Dati Hackerati e Divulgati

Le fonti di grandi set di dati sono molteplici e in continua evoluzione:

• Distributed Denial of Secrets (DDoSecrets): Questa piattaforma si definisce una "biblioteca pubblica" di set di dati divulgati, curata appositamente per giornalisti e ricercatori. Offre sia dataset pubblici che privati (con accesso su richiesta per i giornalisti).
• Canali Telegram di attivisti e siti web di ransomware: Spesso, i dati vengono divulgati direttamente su questi canali o sui siti utilizzati dai gruppi ransomware come "vetrina" in caso di mancato pagamento del riscatto.
• Contatto diretto con hacker: Giornalisti con una reputazione consolidata nel settore possono essere contattati direttamente da hacker che desiderano condividere dati.
• Registri pubblici e dati pubblici online: Anche fonti apparentemente ordinarie possono nascondere grandi quantità di dati utili, come dimostra l'esempio dell'Anti-Defamation League analizzato da Micha Lee.

Affrontare la Sfida dei Big Data

Lavorare con set di dati di grandi dimensioni comporta significative difficoltà pratiche:

• Download: Scaricare centinaia di gigabyte da servizi come Tor può richiedere giorni o settimane, spesso necessitando l'uso di server dedicati.
• Analisi: L'analisi di formati di dati eterogenei (dump di database SQL, dump di email, documenti di Office) richiede software e competenze specializzate, inclusa talvolta la conoscenza della programmazione.
• Autenticazione: Prima di poter utilizzare i dati, è fondamentale verificarne l'autenticità e determinarne l'utilità. Micha Lee ha incrociato gli indirizzi email dei pazienti di America's Frontline Doctors con quelli degli utenti di Gab per autenticare i dati trapelati.

Considerazioni Etiche Cruciali

L'utilizzo di dati ottenuti illegalmente solleva importanti dilemmi etici:

• Interesse pubblico vs. metodo di acquisizione e potenziale danno: I giornalisti devono bilanciare il potenziale beneficio pubblico derivante dalla pubblicazione delle informazioni con le implicazioni etiche del metodo con cui i dati sono stati ottenuti e il potenziale danno alle persone coinvolte.
• Pagamento per i dati hackerati: La prassi di pagare per dati hackerati è controversa. The Intercept, ad esempio, non ha mai pagato fonti per dati hackerati a causa di implicazioni etiche e della frequente disponibilità di dati pubblici. Bellingcat è menzionata come una potenziale eccezione in casi specifici.

Navigare i Rischi Legali

Lavorare con dati hackerati comporta notevoli rischi legali:

• Possesso di materiale illegale: Dati ottenuti dal dark web potrebbero contenere materiale illegale da possedere, come materiale pedopornografico o documenti governativi secretati, il cui semplice possesso può costituire un reato.
• Accuse di cospirazione: Istruire o suggerire a una fonte come evitare di essere scoperta durante la fuga di notizie può comportare rischi legali per il giornalista. Anche chiedere specificamente ulteriori dati potrebbe essere interpretato come cospirazione.
• Violazione delle leggi sulla protezione dei dati: La gestione e la pubblicazione di dati personali devono avvenire nel rispetto delle normative vigenti.
• Giustificazione dell'interesse pubblico: La principale giustificazione legale per la pubblicazione di informazioni sensibili ottenute illegalmente è che essa serva l'interesse pubblico. Questa giustificazione può proteggere i giornalisti da cause per diffamazione. Tuttavia, quando i dati sono stati ottenuti illegalmente, la soglia per la pubblicazione si alza e spesso è necessario dimostrare che la pubblicazione evidenzia potenziali violazioni di legge.

L'Impatto degli Attacchi Informatici sulle Redazioni

L'esperienza del **Guardian**, vittima di un attacco informatico "traumatico" durato tre mesi, evidenzia la **vulnerabilità delle organizzazioni di notizie** e il potenziale impatto sulla loro operatività e sulla volontà di coprire notizie relative a dati hackerati.

Adattare il Giornalismo Investigativo all'Era dei Big Data

La crescente disponibilità di dati richiede un **adattamento delle competenze e delle strategie** del giornalismo investigativo:

• Sviluppo di competenze tecniche: È necessario acquisire competenze nell'analisi dei dati, nell'uso di software specifici e, idealmente, nella programmazione.
• Nuovi metodi di autenticazione e verifica: È fondamentale sviluppare e applicare metodi rigorosi per autenticare e verificare l'utilità di enormi volumi di informazioni.
• Potenziale utilizzo dell'intelligenza artificiale (IA): L'IA potrebbe svolgere un ruolo crescente nell'analisi preliminare dei dati per identificare aree di interesse pubblico, sebbene con cautela data la sua fallibilità.
• Collaborazione: La collaborazione tra giornalisti è essenziale per affrontare la complessità delle inchieste transnazionali basate su dati hackerati.

Lo sviluppo di nuove competenze, l'adozione di strategie rigorose di verifica e la collaborazione sono elementi chiave per navigare con successo in questo nuovo e complesso panorama informativo.

Dati Hackerati | Una Guida Pratica per il Giornalismo Investigativo

Negli ultimi anni, il panorama del giornalismo investigativo ha subito una trasformazione radicale. La sfida principale non è più ottenere informazioni, ma **dare un senso alla quantità enorme di dati**

disponibili, spesso rilasciati da hacker e whistleblower. Questi "tesori" digitali, provenienti da governi, aziende e intermediari finanziari, possono essere miniere d'oro di informazioni di interesse pubblico, ma presentano anche **nuove sfide etiche, legali e logistiche**. Ecco una guida pratica per navigare in questo complesso scenario.

Dove Trovare i Dati Hackerati e Divulgati

Le fonti di grandi set di dati sono molteplici e in continua evoluzione:

• Distributed Denial of Secrets (DDoSecrets): Questa piattaforma si definisce una "biblioteca pubblica" di set di dati divulgati, curata appositamente per giornalisti e ricercatori. Offre sia dataset pubblici che privati (con accesso su richiesta per i giornalisti).
• Canali Telegram di attivisti e siti web di ransomware: Spesso, i dati vengono divulgati direttamente su questi canali o sui siti utilizzati dai gruppi ransomware come "vetrina" in caso di mancato pagamento del riscatto.
• Contatto diretto con hacker: Giornalisti con una reputazione consolidata nel settore possono essere contattati direttamente da hacker che desiderano condividere dati.
• Registri pubblici e dati pubblici online: Anche fonti apparentemente ordinarie possono nascondere grandi quantità di dati utili, come dimostra l'esempio dell'Anti-Defamation League analizzato da Micha Lee.

Affrontare la Sfida dei Big Data

Lavorare con set di dati di grandi dimensioni comporta significative difficoltà pratiche:

• Download: Scaricare centinaia di gigabyte da servizi come Tor può richiedere giorni o settimane, spesso necessitando l'uso di server dedicati.
• Analisi: L'analisi di formati di dati eterogenei (dump di database SQL, dump di email, documenti di Office) richiede software e competenze specializzate, inclusa talvolta la conoscenza della programmazione.
• Autenticazione: Prima di poter utilizzare i dati, è fondamentale verificarne l'autenticità e determinarne l'utilità. Micha Lee ha incrociato gli indirizzi email dei pazienti di America's Frontline Doctors con quelli degli utenti di Gab per autenticare i dati trapelati.

Considerazioni Etiche Cruciali

L'utilizzo di dati ottenuti illegalmente solleva importanti dilemmi etici:

• Interesse pubblico vs. metodo di acquisizione e potenziale danno: I giornalisti devono bilanciare il potenziale beneficio pubblico derivante dalla pubblicazione delle informazioni con le implicazioni etiche del metodo con cui i dati sono stati ottenuti e il potenziale danno alle persone coinvolte.
• Pagamento per i dati hackerati: La prassi di pagare per dati hackerati è controversa. The Intercept, ad esempio, non ha mai pagato fonti per dati hackerati a causa di implicazioni etiche e della frequente disponibilità di dati pubblici. Bellingcat è menzionata come una potenziale eccezione in casi specifici.

Navigare i Rischi Legali

Lavorare con dati hackerati comporta notevoli rischi legali:

• Possesso di materiale illegale: Dati ottenuti dal dark web potrebbero contenere materiale illegale da possedere, come materiale pedopornografico o documenti governativi secretati, il cui semplice possesso può costituire un reato.
• Accuse di cospirazione: Istruire o suggerire a una fonte come evitare di essere scoperta durante la fuga di notizie può comportare rischi legali per il giornalista. Anche chiedere specificamente ulteriori dati potrebbe essere interpretato come cospirazione.
• Violazione delle leggi sulla protezione dei dati: La gestione e la pubblicazione di dati personali

devono avvenire nel rispetto delle normative vigenti.
• Giustificazione dell'interesse pubblico: La principale giustificazione legale per la pubblicazione di informazioni sensibili ottenute illegalmente è che essa serva l'interesse pubblico. Questa giustificazione può proteggere i giornalisti da cause per diffamazione. Tuttavia, quando i dati sono stati ottenuti illegalmente, la soglia per la pubblicazione si alza e spesso è necessario dimostrare che la pubblicazione evidenzia potenziali violazioni di legge.

L'Impatto degli Attacchi Informatici sulle Redazioni

L'esperienza del **Guardian**, vittima di un attacco informatico "traumatico" durato tre mesi, evidenzia la **vulnerabilità delle organizzazioni di notizie** e il potenziale impatto sulla loro operatività e sulla volontà di coprire notizie relative a dati hackerati.

Adattare il Giornalismo Investigativo all'Era dei Big Data

La crescente disponibilità di dati richiede un **adattamento delle competenze e delle strategie** del giornalismo investigativo:

• Sviluppo di competenze tecniche: È necessario acquisire competenze nell'analisi dei dati, nell'uso di software specifici e, idealmente, nella programmazione.
• Nuovi metodi di autenticazione e verifica: È fondamentale sviluppare e applicare metodi rigorosi per autenticare e verificare l'utilità di enormi volumi di informazioni.
• Potenziale utilizzo dell'intelligenza artificiale (IA): L'IA potrebbe svolgere un ruolo crescente nell'analisi preliminare dei dati per identificare aree di interesse pubblico, sebbene con cautela data la sua fallibilità.
• Collaborazione: La collaborazione tra giornalisti è essenziale per affrontare la complessità delle inchieste transnazionali basate su dati hackerati.

Lo sviluppo di nuove competenze, l'adozione di strategie rigorose di verifica e la collaborazione sono elementi chiave per navigare con successo in questo nuovo e complesso panorama informativo.