Un documento vero può raccontare una storia falsa

Maria Cattini | 08/09/2026 | Open source intelligence

Un documento compare online dopo un attacco informatico. Proviene davvero dagli archivi di una pubblica amministrazione. Nomi, date, intestazioni e contenuti sembrano autentici. Qualcuno ne estrae una pagina, la pubblica sui social e aggiunge una conclusione molto più compromettente di ciò che quella pagina dimostra.

La domanda, a quel punto, non è più soltanto se il documento sia vero. Bisogna capire se sia vera **la storia che ci stanno raccontando attraverso quel documento**.

È una distinzione importante nel caso del cyberattacco che ha colpito l'amministrazione di Berlino. Ma è anche una buona regola generale per leggere leak, documenti rubati e materiali che arrivano online dopo un attacco ransomware.

Cosa è successo a Berlino

Un gruppo che si identifica come Rhysida ha rivendicato l'attacco alla rete amministrativa berlinese e ha dichiarato di aver sottratto circa 5,7 terabyte di dati. Il materiale è stato inizialmente messo all'asta con una richiesta di 30 bitcoin. Berlino ha dichiarato che non avrebbe ceduto all'estorsione.

Il 4 settembre le autorità hanno confermato la pubblicazione dei dati rubati. Il giorno successivo la Cancelleria del Senato ha annunciato la costituzione di un'unità centrale incaricata di coordinare l'esame, la verifica e la valutazione dei file, oltre a sostenere le amministrazioni interessate nell'informazione ai cittadini e alle imprese coinvolti. (Berlin)

C'è poi una circostanza che rende il caso particolarmente delicato: il 20 settembre Berlino voterà per il rinnovo della Camera dei deputati della città-Stato. La data è confermata dal Landeswahlleiter, l'autorità elettorale berlinese. (Berlin)

Questa vicinanza temporale, però, non autorizza una scorciatoia.

Non abbiamo elementi sufficienti per affermare che l'attacco ransomware sia stato organizzato per influenzare le elezioni. Confondere una coincidenza temporale con una relazione causale significherebbe fare esattamente ciò da cui questo caso dovrebbe metterci in guardia.

Il problema comincia quando i dati diventano pubblici

Un ransomware ha normalmente un obiettivo molto concreto: estorcere denaro. I criminali possono cifrare i sistemi, sottrarre dati e minacciare di pubblicarli se la vittima non paga.

Quando il materiale viene effettivamente diffuso, però, nasce un secondo problema che non riguarda più soltanto la cybersecurity.

Riguarda l'informazione.

Un archivio rubato può contenere documenti autentici, ma l'autenticità dei singoli file non rende

automaticamente corretta ogni interpretazione costruita a partire da essi.

Immaginiamo un'email autentica di dieci righe. Qualcuno ne pubblica due, eliminando la risposta successiva che ne chiarisce il significato. Oppure mostra una relazione vera del 2024 come se descrivesse la situazione attuale. Ancora: un documento preliminare può essere presentato come una decisione definitiva.

Non serve modificare una sola parola del file originale. Basta modificare il contesto.

È questo il punto più insidioso: **un documento autentico può diventare la prova apparente di un'affermazione falsa**.

Autenticità e verità non sono sinonimi

Davanti a un leak siamo abituati a porci una prima domanda: il file è autentico?

È necessaria, ma non basta.

Occorre distinguere almeno tre livelli.

Il primo riguarda il documento: proviene realmente dall'archivio dal quale si sostiene che provenga?

Il secondo riguarda la sua integrità: quello che vediamo corrisponde al file originale oppure è stato modificato?

Il terzo riguarda l'interpretazione: il documento dimostra davvero ciò che il post, il titolo o l'articolo sostengono?

È perfettamente possibile rispondere sì alle prime due domande e no alla terza.

Ed è proprio questa possibilità a rendere i leak particolarmente difficili da trattare giornalisticamente.

La quantità di documenti può diventare parte della manipolazione

Nel caso berlinese parliamo di terabyte di materiale. Una quantità simile crea un problema pratico: la verifica richiede tempo, mentre la diffusione sui social può essere quasi immediata.

Si produce così una forte asimmetria.

Per pubblicare lo screenshot di un documento bastano pochi secondi. Per stabilirne provenienza, data, autore, contesto, completezza e significato possono servire ore o giorni.

Nel frattempo lo screenshot circola, viene commentato, ripreso da altri account e trasformato in una conclusione politica o giornalistica.

La verifica arriva dopo che la narrazione si è già formata.

Non è un rischio soltanto teorico. Le stesse autorità berlinesi, dopo la pubblicazione dei dati, hanno invitato a non diffondere sui social affermazioni non verificate relative al materiale sottratto. (Berlin)

Sei domande prima di credere a un documento trapelato

Quando un file proveniente da un leak comincia a circolare, il metodo più prudente consiste nel separare il documento dalla narrazione che lo accompagna.

1. Da dove arriva?
Non basta che qualcuno dica che il file appartiene a un determinato leak. Bisogna ricostruirne la

provenienza e capire se esistono elementi che lo colleghino realmente al materiale sottratto.

2. È integro?
Screenshot, estratti e immagini sono particolarmente problematici. Un file autentico può essere tagliato, modificato oppure mostrato solo in parte.

3. Qual è il contesto?
Una frase può assumere un significato diverso leggendo il documento completo, gli allegati o le comunicazioni precedenti e successive.

4. Quando è stato prodotto?
Un documento vecchio presentato come attuale non diventa falso. È falsa l'interpretazione temporale che gli viene attribuita.

5. Chi lo ha scritto?
Una bozza interna, un parere tecnico, una comunicazione informale e una decisione ufficiale non hanno lo stesso valore. Il ruolo dell'autore conta.

6. Dimostra davvero la conclusione che sta circolando?
È probabilmente la domanda più importante. Dobbiamo cercare nel documento la prova dell'affermazione, non limitarci a constatare che il documento esiste.

Anche pubblicare un documento vero comporta responsabilità

C'è infine un altro aspetto che rischia di scomparire nella corsa alla verifica.

Un leak non è un archivio pubblico messo volontariamente a disposizione dei giornalisti. Può contenere dati personali, informazioni riservate e materiale riguardante persone che non hanno alcuna relazione con l'eventuale interesse pubblico della vicenda.

Verificare non significa quindi scaricare e redistribuire indiscriminatamente tutto ciò che compare online.

Prima della pubblicazione occorre chiedersi se quel materiale sia necessario per documentare una notizia, quali conseguenze possa avere sulle persone coinvolte e quali informazioni debbano essere protette. Nel caso di Berlino, le autorità stanno infatti identificando i soggetti interessati dalla fuga di dati e prevedono di informarli secondo le norme applicabili sulla protezione dei dati.

Il caso berlinese, almeno allo stato delle informazioni disponibili, non dimostra l'esistenza di un'operazione per influenzare le elezioni. Dimostra qualcosa di diverso e forse più utile: dopo un ransomware, il problema non finisce necessariamente quando i criminali pubblicano i file.

Per chi legge, verifica o racconta quei documenti, può essere proprio allora che comincia la parte più difficile.

La regola da ricordare è semplice: **prima si verifica il documento, poi si verifica la storia costruita intorno al documento. Sono due verifiche diverse.**
Un documento compare online dopo un attacco informatico. Proviene davvero dagli archivi di una pubblica amministrazione. Nomi, date, intestazioni e contenuti sembrano autentici. Qualcuno ne estrae una pagina, la pubblica sui social e aggiunge una conclusione molto più compromettente di ciò che quella pagina dimostra.

La domanda, a quel punto, non è più soltanto se il documento sia vero. Bisogna capire se sia vera **la storia che ci stanno raccontando attraverso quel documento**.

È una distinzione importante nel caso del cyberattacco che ha colpito l'amministrazione di Berlino. Ma è anche una buona regola generale per leggere leak, documenti rubati e materiali che arrivano online dopo un attacco ransomware.

Cosa è successo a Berlino

Un gruppo che si identifica come Rhysida ha rivendicato l'attacco alla rete amministrativa berlinese e ha dichiarato di aver sottratto circa 5,7 terabyte di dati. Il materiale è stato inizialmente messo all'asta con una richiesta di 30 bitcoin. Berlino ha dichiarato che non avrebbe ceduto all'estorsione.

Il 4 settembre le autorità hanno confermato la pubblicazione dei dati rubati. Il giorno successivo la Cancelleria del Senato ha annunciato la costituzione di un'unità centrale incaricata di coordinare l'esame, la verifica e la valutazione dei file, oltre a sostenere le amministrazioni interessate nell'informazione ai cittadini e alle imprese coinvolti. (Berlin)

C'è poi una circostanza che rende il caso particolarmente delicato: il 20 settembre Berlino voterà per il rinnovo della Camera dei deputati della città-Stato. La data è confermata dal Landeswahlleiter, l'autorità elettorale berlinese. (Berlin)

Questa vicinanza temporale, però, non autorizza una scorciatoia.

Non abbiamo elementi sufficienti per affermare che l'attacco ransomware sia stato organizzato per influenzare le elezioni. Confondere una coincidenza temporale con una relazione causale significherebbe fare esattamente ciò da cui questo caso dovrebbe metterci in guardia.

Il problema comincia quando i dati diventano pubblici

Un ransomware ha normalmente un obiettivo molto concreto: estorcere denaro. I criminali possono cifrare i sistemi, sottrarre dati e minacciare di pubblicarli se la vittima non paga.

Quando il materiale viene effettivamente diffuso, però, nasce un secondo problema che non riguarda più soltanto la cybersecurity.

Riguarda l'informazione.

Un archivio rubato può contenere documenti autentici, ma l'autenticità dei singoli file non rende automaticamente corretta ogni interpretazione costruita a partire da essi.

Immaginiamo un'email autentica di dieci righe. Qualcuno ne pubblica due, eliminando la risposta successiva che ne chiarisce il significato. Oppure mostra una relazione vera del 2024 come se descrivesse la situazione attuale. Ancora: un documento preliminare può essere presentato come una decisione definitiva.

Non serve modificare una sola parola del file originale. Basta modificare il contesto.

È questo il punto più insidioso: **un documento autentico può diventare la prova apparente di un'affermazione falsa**.

Autenticità e verità non sono sinonimi

Davanti a un leak siamo abituati a porci una prima domanda: il file è autentico?

È necessaria, ma non basta.

Occorre distinguere almeno tre livelli.

Il primo riguarda il documento: proviene realmente dall'archivio dal quale si sostiene che provenga?

Il secondo riguarda la sua integrità: quello che vediamo corrisponde al file originale oppure è stato modificato?

Il terzo riguarda l'interpretazione: il documento dimostra davvero ciò che il post, il titolo o l'articolo sostengono?

È perfettamente possibile rispondere sì alle prime due domande e no alla terza.

Ed è proprio questa possibilità a rendere i leak particolarmente difficili da trattare giornalisticamente.

La quantità di documenti può diventare parte della manipolazione

Nel caso berlinese parliamo di terabyte di materiale. Una quantità simile crea un problema pratico: la verifica richiede tempo, mentre la diffusione sui social può essere quasi immediata.

Si produce così una forte asimmetria.

Per pubblicare lo screenshot di un documento bastano pochi secondi. Per stabilirne provenienza, data, autore, contesto, completezza e significato possono servire ore o giorni.

Nel frattempo lo screenshot circola, viene commentato, ripreso da altri account e trasformato in una conclusione politica o giornalistica.

La verifica arriva dopo che la narrazione si è già formata.

Non è un rischio soltanto teorico. Le stesse autorità berlinesi, dopo la pubblicazione dei dati, hanno invitato a non diffondere sui social affermazioni non verificate relative al materiale sottratto. (Berlin)

Sei domande prima di credere a un documento trapelato

Quando un file proveniente da un leak comincia a circolare, il metodo più prudente consiste nel separare il documento dalla narrazione che lo accompagna.

1. Da dove arriva?
Non basta che qualcuno dica che il file appartiene a un determinato leak. Bisogna ricostruirne la provenienza e capire se esistono elementi che lo colleghino realmente al materiale sottratto.

2. È integro?
Screenshot, estratti e immagini sono particolarmente problematici. Un file autentico può essere tagliato, modificato oppure mostrato solo in parte.

3. Qual è il contesto?
Una frase può assumere un significato diverso leggendo il documento completo, gli allegati o le comunicazioni precedenti e successive.

4. Quando è stato prodotto?
Un documento vecchio presentato come attuale non diventa falso. È falsa l'interpretazione temporale che gli viene attribuita.

5. Chi lo ha scritto?
Una bozza interna, un parere tecnico, una comunicazione informale e una decisione ufficiale non hanno lo stesso valore. Il ruolo dell'autore conta.

6. Dimostra davvero la conclusione che sta circolando?
È probabilmente la domanda più importante. Dobbiamo cercare nel documento la prova dell'affermazione, non limitarci a constatare che il documento esiste.

Anche pubblicare un documento vero comporta responsabilità

C'è infine un altro aspetto che rischia di scomparire nella corsa alla verifica.

Un leak non è un archivio pubblico messo volontariamente a disposizione dei giornalisti. Può contenere dati personali, informazioni riservate e materiale riguardante persone che non hanno alcuna relazione con l'eventuale interesse pubblico della vicenda.

Verificare non significa quindi scaricare e redistribuire indiscriminatamente tutto ciò che compare online.

Prima della pubblicazione occorre chiedersi se quel materiale sia necessario per documentare una notizia, quali conseguenze possa avere sulle persone coinvolte e quali informazioni debbano essere protette. Nel caso di Berlino, le autorità stanno infatti identificando i soggetti interessati dalla fuga di dati e prevedono di informarli secondo le norme applicabili sulla protezione dei dati.

Il caso berlinese, almeno allo stato delle informazioni disponibili, non dimostra l'esistenza di un'operazione per influenzare le elezioni. Dimostra qualcosa di diverso e forse più utile: dopo un ransomware, il problema non finisce necessariamente quando i criminali pubblicano i file.

Per chi legge, verifica o racconta quei documenti, può essere proprio allora che comincia la parte più difficile.

La regola da ricordare è semplice: **prima si verifica il documento, poi si verifica la storia costruita intorno al documento. Sono due verifiche diverse.**