proofpoint.

# Riepilogo sulle minacce: il ransomware

## In breve

**Descrizione:**

Il ransomware codifica i dati critici o blocca agli utenti l'accesso ai rispettivi dispositivi fino a quando non pagano un riscatto all'aggressore, in genere un'organizzazione criminale.

**Strumenti utilizzati:**

Cryptolocker, WannaCry, Bad Rabbit, Cerber, Crysis, CryptoWall, GoldenEye, Jigsaw, Locky, Petya, Conti, Sodinokibi e Ryuk

**Origine:**

1989, AIDS Trojan creato da Joseph Popp. Popp inviò 20.000 dischetti infetti etichettati "AIDS Information-Introductory Diskettes" ai partecipanti della conferenza internazionale sull'AIDS dell'Organizzazione Mondiale della Sanità e creò quello che ora è stato battezzato come il primo attacco ransomware al mondo.

**Tipi:**

- **Ransomware crypto**
  I criminali informatici cifrano i file presenti su un computer, impedendo così all'utente di accedervi.
- **Ransomware locker**
  Malware che blocca il computer della vittima, impedendole di accedere al proprio dispositivo fino al pagamento di un riscatto.
- **"Scareware"**
  Questo malware induce le vittime a credere di essere state infettate da un ransomware e le spinge a inviare un pagamento all'aggressore. Sebbene non sia tecnicamente un ransomware, lo scareware può avere lo stesso effetto sulle vittime.

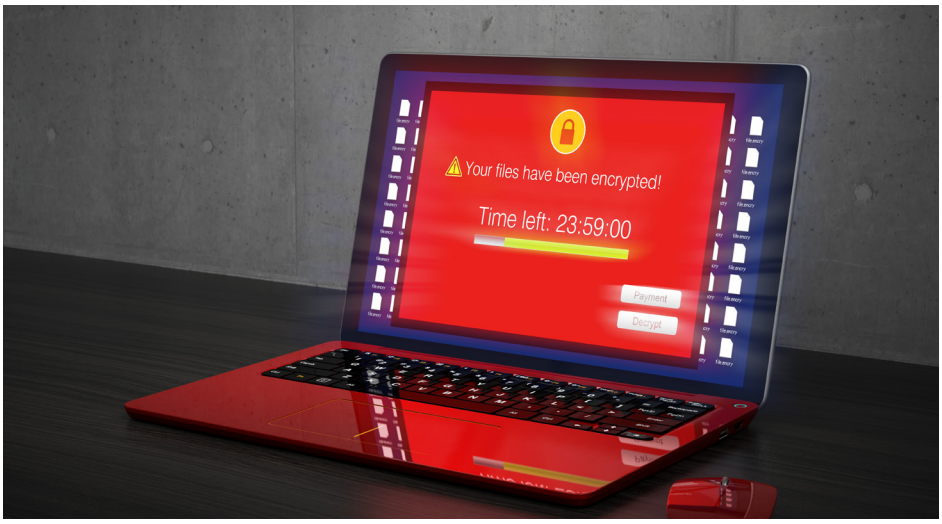
**Fattori di rischio:**

- Software e sistemi vulnerabili
- Nessun backup facilmente accessibile
- Sicurezza informatica inefficace o inesistente
- Utenti non formati e vulnerabili

**Possibili danni:**

- Perdita di denaro
- Perdita di dati sensibili o proprietari
- Potenziale danno alla reputazione
- Interruzione dell'attività e perdita di produttività

Il ransomware, così chiamato per via del riscatto (ransom in inglese) chiesto alla vittima dopo il blocco dei file, è un problema molto serio per tutte le organizzazioni moderne. È uno degli attacchi informatici più dannosi presente oggi, perché rischia di causare il fallimento delle aziende colpite, costringe gli ospedali a rifiutare i pazienti e blocca intere amministrazioni pubbliche. Il modo migliore per gestire il ransomware è impedire che si insinui nel tuo ambiente. Qui puoi trovare un'introduzione a questa minaccia in rapida ascesa.




## Attacchi ransomware divenuti famosi

### Universal Health Services perde 67 milioni di dollari nell'attacco ransomware Ryuk

Un attacco ransomware sferrato contro Universal Health Services (UHS) è costato all'azienda circa 67 milioni di dollari a causa dei tempi di inattività registrati e delle spese correlate. L'organizzazione sanitaria Fortune 500 conta decine di migliaia di dipendenti negli Stati Uniti e nel Regno Unito e un fatturato annuale superiore a 10 miliardi di dollari.[1]

### UCSF paga un riscatto di 1,14 milioni di dollari per recuperare i dati delle ricerche

Gli aggressori hanno colpito l'università bloccando i sistemi informatici della UCSF School of Medicine. Gli amministratori hanno reagito rapidamente tentando di isolare l'infezione e di bloccare una serie di sistemi che hanno impedito al ransomware di viaggiare verso la rete principale della UCSF e causare danni maggiori.[2]

### I profitti di Cognizant hanno subito perdite per 50-70 milioni di USD per via del ransomware

Il fornitore di servizi IT Cognizant è stato vittima di un attacco ransomware nell'aprile 2020 che ha compromesso i suoi profitti del secondo trimestre. A seguito dell'attacco, la società ha dovuto sostenere costi legali, di consulenza e di altra natura per eseguire indagini sull'incidente, ripristinare il servizio e bonificare i sistemi.[3]

1 Phil Muncaster (*Infosecurity*). "Universal Health Services Estimates $67 Million in Ransomware Losses." (Universal Health Services perde 67 milioni di dollari a causa del ransomware) Marzo 2021.
2 Charlie Osborne (*ZDNet*). "University of California SF pays ransomware hackers $1.14 million to salvage research." (La University of California SF paga agli hacker 1,14 milioni di dollari per recuperare i dati delle ricerche) Giugno 2020.
3 Catalin Cimpanu (*ZDNet*). "Cognizant expects to lose between $50m and $70m following ransomware attack." (Cognizant stima una perdita di 50-70 milioni di dollari a causa di un attacco ransomware) Maggio 2020.

### Attacco ransomware interrompe la fornitura di carburante degli Stati Uniti

A maggio 2021 uno dei più grandi oleodotti degli Stati Uniti si è spento a causa di un attacco ransomware, provocando l'interruzione delle operazioni in un sistema di oltre 8850 km che provvede a quasi la metà della fornitura totale di carburante alla costa orientale degli USA.[4] L'operatore dell'oleodotto ha pagato agli aggressori 4,4 milioni di dollari per sbloccare i dati, ma "alla fine non è stato sufficiente per ripristinare immediatamente i sistemi dell'oleodotto".[5]

### La più grande azienda al mondo di carne confezionata sospende la produzione di carne bovina dopo un attacco ransomware

L'azienda brasiliana ha spento gli impianti di confezionamento della carne in Colorado, Iowa, Minnesota, Pennsylvania, Nebraska e Texas a causa di un attacco che, secondo quanto sostenuto dai funzionari statunitensi, sembra essere partito dalla Russia.[6] In un comunicato stampa, la società ha dichiarato di avere individuato l'attacco sulle sue reti informatiche in Nord America e Australia. Fortunatamente, i server di backup non sono stati colpiti.[7]

## Caratteristiche di un attacco ransomware

Nel corso di oltre tre decenni, il ransomware si è evoluto in una delle minacce informatiche più pericolose di sempre. Le valute digitali come i Bitcoin hanno agevolato i criminali informatici nella riscossione dei riscatti. Inoltre, gli aggressori stanno diventando più abili nel colpire sistemi vecchi e obsoleti.

**Ecco le fasi con cui si manifestano molti attacchi ransomware:**

**1. Distribuzione |** Gli aggressori inducono gli utenti ad accedere al software dannoso utilizzando email di phishing, social engineering, falsi siti web con link dannosi, dispositivi di archiviazione esterni infetti come le chiavette USB. In molti casi, il ransomware è un payload secondario distribuito a sistemi già compromessi.

**3. Preparazione |** Il payload del ransomware distribuito dal file si nasconde e si insinua all'interno del sistema.

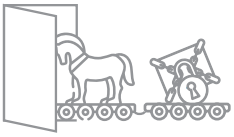
**5. Avviso di riscatto |** Viene visualizzato un avviso per la vittima in cui si richiede un pagamento per il rilascio dei file.


**2. Infezione |** L'utente scarica inconsapevolmente un file eseguibile chiamato loader (o downloader) che installa il ransomware.

**4. Scansione e codifica |** Il malware scansiona il sistema e la rete e codifica i file.

I criminali informatici hanno poi scoperto che la maggior parte delle vittime di ransomware dispone di un backup dei dati e si rifiuta di pagare il riscatto, per questo motivo si sono evoluti. Iniziano rubando e cifrando i file, poi minacciano di rendere pubblici i dati sottratti. Le informazioni potrebbero essere estremamente sensibili o personali e renderle di pubblico dominio potrebbe avere conseguenze devastanti. A ciò si aggiunge il fatto che i ceppi di ransomware sofisticati sono in grado di cercare e cifrare anche i backup.

4 David E. Sanger, Clifford Krauss e Nicole Perlroth (*The New York Times*). "Cyberattack Forces a Shutdown of a Top U.S. Pipeline." (Attacco informatico costringe alla chiusura il più grande oleodotto degli USA) Maggio 2021.
5 Collin Eaton e Dustin Volz (*The Wall Street Journal*). "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom." (Il CEO di Colonial Pipeline spiega perché ha pagato agli hacker un riscatto di 4,4 milioni di dollari) Maggio 2021.
6 Jacob Bunge (*The Wall Street Journal*). "Meat Buyers Scramble After Cyberattack Hobbles JBS." (Consumatori di carne in agitazione dopo che un attacco informatico mette in ginocchio JBS) Giugno 2021.
7 Hamza Shaban, Ellen Nakashima e Rachel Lerman (*The Washington Post*). "JBS, world's largest meat processor, shut down U.S. beef plants amid cyberattack." (JBS, la principale azienda di carne confezionata, chiude gli impianti USA a causa di un attacco informatico) Giugno 2021.



### COME SI SONO EVOLUTI GLI ATTACCHI RANSOMWARE

Una volta il ransomware era un payload primario in campagne email dannose, ma ora assume sempre più spesso le sembianze di un'infezione secondaria.

I criminali informatici che distribuiscono trojan e altri tipi di malware consentono ai gruppi di ransomware di utilizzare le backdoor nei sistemi infetti in cambio di una quota dei profitti.

Questo significa che, per la maggior parte delle aziende, la prima linea di difesa contro il ransomware è implementare una protezione valida contro l'infezione iniziale. In altre parole, bloccando il loader si blocca il ransomware.

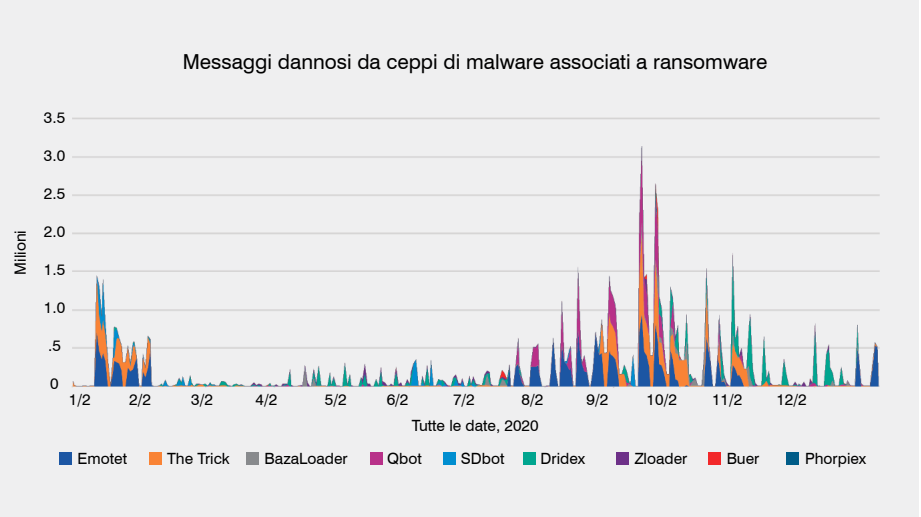
## Osservazioni della ricerca

Il ransomware viene comunemente distribuito come infezione secondaria dopo che un sistema è stato compromesso per la prima volta attraverso un'email dannosa. Dalle nostre osservazioni, e da quelle di altri ricercatori, abbiamo dedotto che molti dei ceppi di malware più prolifici sono strettamente associati a successive infezioni di ransomware.

Qui riportiamo un elenco dei ceppi di malware comuni e di ransomware più strettamente associato ad essi.

| MALWARE/DOWNLOADER | RANSOMWARE ASSOCIATO |
|---|---|
| Emotet | Ryuk |
| The Trick | Conti |
| Dridex | BitPaymer/DoppelPaymer |
| Qbot | Egregor |
| SDBbot | Clop |
| ZLoader | Egregor e Ryuk |
| Buer (Buer Loader) | Ryuk |
| Phorphiex/Trik | Avaddon |

Emotet, The Trick, Dridex e Qbot sono stati tra i malware più prolifici che abbiamo registrato nel 2020, con volumi costanti presenti per tutto l'anno e picchi significativi in autunno.




## Sempre più organizzazioni cedono al ricatto, con risultati contrastanti

Secondo lo State of Phish Report del 2021 di Proofpoint, il 68% delle organizzazioni statunitensi intervistate ha dichiarato di aver pagato un riscatto nel 2020. Un dato questo che è il doppio della media globale. Per contro, il 41% delle organizzazioni spagnole ha rifiutato di pagare il riscatto dopo la diffusione dell'infezione. Su scala globale, queste aziende sono state considerate le meno disposte a negoziare con i criminali informatici.

Dopo aver pagato un riscatto una tantum, nel 78% dei casi le organizzazioni francesi sono state in grado di riottenere l'accesso ai propri dati. Seguono al secondo posto gli Stati Uniti con il 76%.

Stando a quanto dichiarato dagli esperti di Infosec, nel 2020 il 34% delle organizzazioni infettate ha scelto di pagare il riscatto. Il 32% è stato infettato ma non ha pagato il riscatto e il 34% ha dichiarato di non avere subito attacchi ransomware.

# Come proteggere l'organizzazione

Il modo migliore per affrontare il ransomware è quello di evitarlo.

## Prima dell'attacco

Dovrai partire dal presupposto che prima o poi sarai vittima di ransomware. Il piano successivo dovrebbe includere prevenzione, rilevamento e risposta. Ad esempio:

- Eseguire il backup dei dati critici, testare le procedure di ripristino dei dati e mantenere i backup segmentati dai file system primari
- Aggiornare e applicare le patch ai sistemi
- Formare e istruire gli utenti
- Investire in soluzioni di sicurezza incentrate sulle persone
- Applicare la segmentazione della rete per limitare la diffusione
- Decidere prima dell'attacco se, quanto e in quali circostanze l'organizzazione è disposta a pagare un riscatto in caso di attacco

## Durante l'attacco

Se sei vittima di un attacco, devi puntare a prevenire ulteriori danni e avere già un piano di risposta. Ad esempio:

- Contattare le forze dell'ordine
- Scollegarsi dalla rete
- Determinare la portata del problema in base alla threat intelligence
- Organizzare una risposta
- Applicare la segmentazione della rete per limitare la diffusione
- Cercare altre vulnerabilità, malware e compromissioni del sistema che probabilmente sono una conseguenza del ransomware
- Non contare su strumenti gratuiti di decodifica del ransomware
- Ripristinare i dati critici: cercare qualsiasi malware che possa essere stato salvato con altri dati

## Dopo l'attacco

All'indomani di un attacco ransomware, sarà necessario prendere provvedimenti per ripristinare e risolvere i problemi causati dall'incidente. Ad esempio:

- Pulizia e bonifica
- Revisione della sicurezza post-mortem
- Valutare la consapevolezza degli utenti
- Controlli basati sul rischio e incentrati sulle persone
- Valutare nuovamente la propria posizione di sicurezza e allineare gli investimenti in base alle aree di maggior rischio

## È corretto pagare il riscatto?

Pagare un riscatto finanzia l'attività criminale. Ciononostante, le conseguenze di un attacco possono essere gravi sia per l'azienda che per i suoi clienti. Non esiste una risposta giusta a questa domanda.

Le organizzazioni devono considerare alcuni fattori prima di decidere quale linea d'azione seguire:

- Sicurezza dei clienti e dei dipendenti
- Tempo e risorse necessarie per il ripristino
- Responsabilità verso gli azionisti in relazione all'interruzione delle attività aziendali
- Tipo di attività criminale che il pagamento potrebbe finanziare

Qualunque sia la decisione, dovrebbe essere presa prima di un attacco, quando i dirigenti non sono sotto pressione per via di una scadenza imminente e di un'attività commerciale gravemente danneggiata. Oltre a decidere se l'organizzazione pagherà o meno un riscatto, i dirigenti dovrebbero anche stabilire quanto sono disposti a sborsare e a quali condizioni. È inoltre importante ricordare che alcuni pagamenti, ad esempio quelli a favore di criminali inseriti negli elenchi di sanzioni degli Stati Uniti, possono essere illegali.

## PER SAPERNE DI PIÙ

Il modo migliore per fermare il ransomware è la prevenzione proattiva. Un solido piano di prevenzione del ransomware coinvolge la sicurezza incentrata sulle persone. È necessario istruire i propri dipendenti attraverso una formazione basata su tecniche di attacco del mondo reale. In questo modo è possibile bloccare il ransomware e i downloader di malware che prendono di mira le persone. Questo piano aiuta a rispondere rapidamente e a prendere le misure necessarie prima che la situazione si aggravi.

Per saperne di più su come fermare in modo efficace il ransomware, è possibile scaricare la nostra Ransomware Survival Guide

Per ulteriori informazioni, visitare la pagina **proofpoint.com/it**.