Ransomware: troppe vittime, poche soluzioni

La riscoperta di un attacco proficuo

Noti già da tempo, questi attacchi trovano largo impiego per il loro aspetto lucrativo e per la loro propagazione rapida e devastante. Oggigiorno, assistiamo a un aumento costante di queste minacce: secondo quanto indicato dall'ANSSI, **tra il 2020 e il 2021 il numero di attacchi è cresciuto del 37%**. Analogamente, la stessa tendenza costante si osserva con il Ransomware as a Service (RaaS).

Il ransomware è un tipo di malware che rende inaccessibili i dati, chiedendo un riscatto.

La prima categoria, il classico ransomware denominato "poliziesco", **blocca il desktop** (chiamato Browlock) e paralizza il computer.

Della seconda fanno parte i più dannosi Crypto-ransomware o Cryptoware, **che criptano i documenti presenti sul computer** della vittima rendendoli illeggibili in assenza della chiave di decrittazione in possesso del cyber criminale, il quale richiede poi un riscatto in cambio di tale chiave.

In questo caso, che è anche più recente, il malware **esfiltra i dati e minaccia di divulgarli** in cambio di un ulteriore pagamento.

7.000 euro

Costo medio di un attacco informatico

Fonte: L'usine digitale

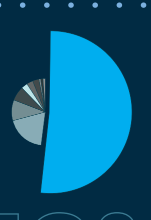
SECONDO DATOS101 **GLI ATTACCHI RANSOMWARE SONO AUMENTATI DEL 253%**

UNA FAMIGLIA ATTIVA E DIVERSIFICATA

...
GPcode (.AG, .AK)
LOCKBIT 2.0
TROJ.RANSOM.A
Archiveus
Krotten
RSA4096
Cerber
Cryzip
MayArchive
Petya
CryptoLocker
TorrentLocker
Cryptowall
TeslaCrypt
Locky Ransomware
KeRanger
CTB-Locker
WinLock
Reveton
Winwebsec
...

SIAMO **TUTTI PREOCCUPATI**

Clienti privati e aziende di qualsiasi settore e dimensione



Il 52% delle vittime sono PMI

Tutti i sistemi operativi sono vulnerabili

KERANGER
IL PRIMO RANSOMWARE CHE COLPISCE I SISTEMI MACOSX (2016)

CTB-LOCKER
(VARIANTE)
PRENDE DI MIRA I SERVER WEB IN AMBIENTE GNU/LINUX

> ***L'obiettivo di sabotare le infrastrutture critiche è tuttora una minaccia costante.***

In un rapporto, Hiscox rivela **che quasi i due terzi delle vittime di ransomware sono state oggetto di phishing (65%), superando di gran lunga il furto di credenziali (39%).**

COMMUNITY DI CRIMINALI
Attualmente le varie campagne di ransomware non sono più gestite da un solo gruppo, **ma da diversi gruppi di cyber criminali**.

LE CAMPAGNE SONO MIRATE
Un esempio significativo: Locky
Il ramsonware Locky prende di mira le aziende, diffondendosi attraverso campagne di email malevole (email di fatture false, comunicazioni da parte di aziende di telefonia mobile, ecc.).**L'efficacia di questi attacchi è quindi potenziata dalla personalizzazione.**

I CRYPTOWARE
Decifrare i ransomware sta diventando sempre più difficile, con una conseguente riduzione delle possibilità di recupero dei dati senza il pagamento di un riscatto.

In pochissimo si è assistito a un notevole aumento della lunghezza e della resistenza delle chiavi.

CONSTATAZIONI
Questo tipo di attacco è in costante aumento (nuovi attacchi o varianti).

CREARE IL PROPRIO RANSOMWARE SENZA CONOSCENZE TECNICHE

RANSOMWARE-AS-A-SERVICE

Al giorno d'oggi chiunque può accedervi perché ***sul Dark Web si può generare codice malevolo da utilizzare a piacimento.***

COME FUNZIONA?

Con strumenti passo-passo molto semplici, il cyber criminale può creare rapidamente il proprio ransomware. Remunera il fornitore di questo servizio pagandogli il 25% delle transazioni effettuate dalla campagna.

Fase 1
Personalizzazione

1. Il criminale sceglie **il tipo di attacco**
   - [x] Blocco
   - [x] Crittografia
   - [ ] Conto alla rovescia
2. quindi redige **il messaggio**
   Messaggio
   I vostri dati personali sono stati criptati
   L'accesso alla postazione di lavoro è stato bloccato. Per recuperare i dati, effettuare un pagamento di 200€ a questo indirizzo:
3. poi fornisce **le informazioni di pagamento**
   bitcoin

Fase 2
Creazione

4. Il servizio **prepara il malware** secondo le scelte effettuate
5. Il codice è **pronto per l'uso**
   </>

Fase 3
Diffusione

SI COMINCIA!
Per la propagazione, il ransomware impiegherà diversi metodi come ad esempio un "exploit kit" per sfruttare una vulnerabilità.

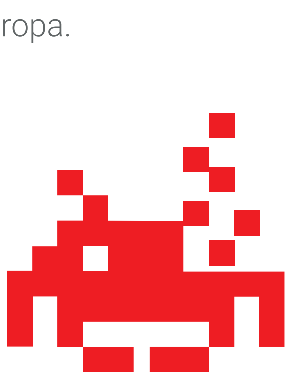
...

LOCKBIT 2.0

LockBit è un gruppo di criminali informatici che opera secondo un modello di ransomware-as-a-service (RaaS).

Attualmente, il ransomware LockBit 2.0 continua ad adattarsi ed evolversi con attacchi mirati negli Stati Uniti, in Canada ed in Europa.

Le varianti più recenti hanno adottato il modello della doppia estorsione: per prima cosa localizzare ed esfiltrare i dati prima di crittografare i sistemi.



PER MAGGIORI INFORMAZIONI

Scoprite in che modo l'attacco LockBit minaccia le infrastrutture attraverso **l'esfiltrazione e la crittografia dei dati.**

E la risposta di Stormshield con il sistema di protezione **anti ransomware della soluzione Endpoint Security Evolution.**

I RANSOMWARE NON SI DIFFONDONO SOLO VIA E-MAIL

- un sito web compromesso o malevolo,
- una chiavetta USB,
- l'installazione di un software/applicazione da una fonte non attendibile
- i social network (che facilitano il social engineering)...

COMPUTER WORM
MALWARE E-MAIL
FILELESS ATTACK
HACKER
DISPOSITIVI INFETTI
VULNERABILITÀ DEI SOFTWARE
TROJAN

UNA SOLUZIONE CONTRO I RANSOMWARE

ESISTE

STORMSHIELD
Endpoint Security Evolution

Questa soluzione proattiva impedisce l'esecuzione del malware sul proprio computer e/o lo sfruttamento di vulnerabilità.

Stormshield Endpoint Security Evolution, grazie alla sua tecnologia di identificazione dei comportamenti caratteristici dei malware, è in grado di bloccare il ransomware prima ancora che venga individuato dalla community di sicurezza informatica.

Your **company** With Stormshield Endpoint Security Evolution
is protected against ransomware

Per maggiori informazioni:
www.stormshield.com/products-services/products/endpoint-protection/

ALCUNI CONSIGLI UTILI
Per proteggervi dai ransomware

Attenzione
alle e-mail sospette che contengono allegati

Eseguire
regolarmente copie di backup

Aggiornare
le applicazioni, i plugin e i sistemi operativi