RANSOMWARE E CRYPTOLOCKER

+493%

ATTACCHI RANSOMWARE

crescita negli ultimi 3 anni (ENISA)

22 gg

TEMPO MEDIO

di interruzione operativa post-attacco

95%

VETTORE EMAIL

degli attacchi inizia da phishing/allegati

EMILIA INFORMATICA
let's connect

I ransomware moderni non si limitano a cifrare i dati: esfiltrano informazioni riservate e minacciano la pubblicazione per massimizzare la pressione sul bersaglio (doppia estorsione).

Emilia Informatica progetta strategie di difesa a più livelli — backup immutabile, endpoint detection, filtraggio perimetrale e formazione degli utenti — per ridurre al minimo la superficie d'attacco e garantire il ripristino rapido in caso di incidente.

ACCREDIA · L'ENTE DI ACCREDITAMENTO ·

UNI EN ISO 9001:2015
CERTIQUALITY
SISTEMA DI GESTIONE QUALITÀ CERTIFICATO

I ransomware rappresentano oggi la minaccia cyber più diffusa e dannosa per le organizzazioni di ogni dimensione. CryptoLocker e le sue varianti moderne (LockBit, BlackCat, Cl0p) sono trojan di tipo ransomware che, una volta eseguiti, cifrano tutti i file accessibili — locali, su share di rete e backup collegati — rendendoli completamente inutilizzabili. Per sbloccarli viene richiesto il pagamento di un riscatto in criptovaluta.

Le varianti più recenti adottano la tecnica della doppia estorsione: oltre a cifrare i dati, li esfiltrano preventivamente e minacciano di pubblicarli online se il riscatto non viene pagato entro la scadenza. Questo rende inefficace il solo ripristino da backup come contromisura, e aumenta enormemente il danno reputazionale e legale per le vittime.

Il vettore di infezione principale rimane la posta elettronica con allegati malevoli o link a siti compromessi (phishing e spear-phishing). I file eseguibili vengono mascherati con doppie estensioni (es. "fattura.pdf.exe") o veicolati tramite macro Office, script PowerShell e file LNK. In alcuni casi l'attacco sfrutta vulnerabilità RDP esposte su internet o credenziali compromesse acquistate sul dark web.

Una volta avviato, il malware contatta i server C2 (Command & Control) dell'attaccante per ricevere la chiave di cifratura, poi procede sistematicamente a cifrare documenti, database, immagini e backup collegati. L'esecuzione può non essere bloccata dagli antivirus tradizionali basati su signature perché le varianti zero-day non sono ancora presenti nei database di rilevamento.

La prevenzione richiede un approccio multi-livello: dalla formazione degli utenti al rilevamento comportamentale degli endpoint, dal filtraggio delle email alla segmentazione di rete, fino a strategie di backup immutabile con retention estesa e piani di Disaster Recovery testati regolarmente.

MITIGARE IL RISCHIO

Consapevolezza e formazione degli utenti

Gli utenti dovrebbero prestare massima attenzione agli allegati email, specialmente file ZIP, .cab, .exe, .lnk, .js, .vbs e documenti Office con macro. Le simulazioni di phishing periodiche aumentano significativamente la capacità di riconoscere tentativi di inganno. Nessun ransomware moderno può fare grandi danni senza l'esecuzione iniziale da parte di un utente.

Endpoint Detection & Response (EDR/XDR)

Le soluzioni EDR/XDR moderne analizzano il comportamento degli eseguibili in tempo reale, bloccando minacce zero-day non ancora presenti nelle signature tradizionali. ESET PROTECT offre una piattaforma unificata di gestione della sicurezza endpoint: protezione multi-layer contro ransomware e malware avanzati, LiveGuard (sandbox cloud) per l'analisi di file sospetti, protezione degli accessi RDP, monitoraggio delle vulnerabilità delle applicazioni installate e visibilità centralizzata su tutti i dispositivi aziendali da un'unica console cloud. Supporta Windows, macOS, Linux, Android e iOS.

Soluzione di Endpoint Security & EDR:

ESET PROTECT

Protezione perimetrale avanzata (NGFW / UTM)

I Next-Generation Firewall ispezionano il traffico in profondità (Deep Packet Inspection), bloccando comunicazioni verso server C2, download di payload e traffico cifratio anomalo. Fortinet FortiGate integra firewall, IPS, antivirus gateway, web filtering, sandboxing cloud (FortiSandbox) e SD-WAN in un'unica piattaforma ad alte prestazioni. FortiSOC e FortiAnalyzer forniscono visibilità e correlazione degli eventi di sicurezza su tutta l'infrastruttura, con alerting in tempo reale e risposta automatizzata agli incidenti — fondamentale per rilevare movimenti laterali prima che il ransomware si propaghi.

Soluzione UTM / NGFW:

Fortinet FortiGate

Data Protection e backup immutabile

Una strategia di backup robusta è l'ultima linea di difesa contro il ransomware. Arcserve Unified Data Protection offre backup agent-based e agentless per ambienti fisici, virtuali (VMware, Hyper-V), cloud (Azure, AWS) e SaaS (Microsoft 365). Supporta la creazione di snapshot immutabili con retention configurabile, replica offsite automatica, deduplicazione e ripristino granulare a livello di file, VM o bare metal. Il Recovery Point Objective (RPO) può scendere a pochi minuti, garantendo la continuità operativa anche dopo un attacco ransomware su larga scala.

Soluzione di Data Protection:

Arcserve UDP

Sicurezza email e anti-phishing avanzata

L'analisi del contenuto di email e allegati a livello gateway è essenziale per bloccare ransomware prima che raggiungano la casella dell'utente. Libraesva Email Security Gateway utilizza motori anti-spam e anti-malware multipli, analisi URL in tempo reale (URL Sandbox), sandboxing degli allegati con detonazione controllata, protezione avanzata da phishing e BEC (Business Email Compromise), e filtri anti-spoofing (SPF, DKIM, DMARC). È disponibile sia on-premise che in modalità cloud-hosted, con integrazione nativa per Microsoft 365 e Google Workspace.

Soluzione di Mail Security:

Libraesva Email Security

Per maggiori informazioni sulle soluzioni, i consulenti tecnici di Emilia Informatica sono a vostra disposizione.