www.cyberintuition.it
info@cyberintuition.it

TECNOLOGIA RAPTOR

La soluzione RaPToR (Ransomware Prevention Toolkit and Rescue) di Cyber Intuition, di seguito per brevità “Raptor o software”, è una piattaforma software di sviluppo interamente italiano che si pone come obiettivo la tutela dei dati, presenti all’interno delle memorie di massa della macchina sulla quale il software è installato, da infezioni locali.

RaPToR intercetta l'esecuzione dei Ransomware analizzando il comportamento dei processi in esecuzione della macchina e impedendo, ove possibile, la crittografia dei dati utente e di sistema e permettendo il recupero di eventuali dati crittografati mediante il ripristino da copie di sicurezza generate costantemente.

FUNZIONALITÀ

RaPToR previene la perdita dei dati dovuti alla crittografia da parte dei Ransomware e ne permette l’eventuale recupero da backup con tecnologia Shadow Copy create automaticamente a cadenza giornaliera o personalizzata qualora una nuova tipologia di Ransomware riesca a bypassare i sistemi di riconoscimento del motore comportamentale. Tale funzionalità, vero e proprio core del software, permette di ridurre al minimo la presenza di falsi positivi.

Le funzionalità di base del software si compongono di due moduli distinti con compiti ben definiti:

- **Motore di analisi comportamentale**, con funzionalità di Memory Dump e Honeypot
- **Funzionalità di tutela e ripristino dei dati**

Tali funzionalità sono presenti all’interno di una componente agent, snella e leggera, da installarsi sulle macchine (client e server), che permette il monitoraggio dei processi e delle loro attività, e la rilevazione e il blocco degli attacchi. Le funzionalità offerte a copertura dei requisiti sono di seguito elencate.

- **Rilevazione dei dati che transitano nell'organizzazione**, ovunque siano archiviati, e valutazione del rischio di perdita di dati (DLP Risk Assessment).

  La piattaforma è in grado di monitorare e analizzare gli accessi che vengono effettuati sui dati da parte dei processi della macchina e degli utenti relativi a questi, classificando i processi stessi come malevoli e valutando real-time il rischio di perdita di informazioni; Questo viene fatto assegnando dei punteggi di rischio ai processi monitorati. Al superamento delle soglie predefinite vengono attivate le procedure di protezione.
- **Analisi e classificazione dei dati** (DLP Information classification)

  La piattaforma è in grado di analizzare e classificare i dati di interesse dei processi di tipo ransomware e suggerire una lista di aree/cartelle considerate ad alto rischio, che potrebbero contenere dati sensibili per l’utente.
- **Possibilità di creare regole predefinite per la protezione dei dati**, identificando i sistemi in cui sono memorizzati (ad esempio porte USB, CD, DVD, porte COM & LPT, dischi rimovibili, dispositivi di acquisizione immagini, modem) per assicurarsi che siano usati in conformità con le politiche di privacy e sicurezza (DLP data at rest)

  La piattaforma è in grado di identificare l’accesso ai dati sensibili ovunque essi risiedano (porte USB, CD, DVD, porte COM & LPT, dischi rimovibili) e configurare delle policy. Esempi di configurazioni che possono essere eseguite tramite la piattaforma sono:
  - Indicazione di azioni automatiche in conseguenza di un attacco rilevato (es, shutdown temporizzato e forzato della macchina, riavvio esclusivo in modalità provvisoria, semplice notifica di avvenuta infezione);
  - Configurazione della cartella di destinazione utilizzata per il salvataggio dei file di dump;
  - Indicazione di cartelle specifiche classificate dall'utente come ad alto rischio.
- **Generazione automatica di alert** nel caso in cui vengano violate le policy di sicurezza definite. La piattaforma è in grado di generare alert in real-time in conseguenza di una rilevazione di possibile infezione ransomware. Gli alert possono essere visualizzati accedendo alla console.

- Possibilità di **generare report di sintesi** (executive summary) **e di dettaglio** (technical report) sulle analisi svolte. E' possibile generare report di sintesi e di dettaglio tramite le funzionalità della console. In particolare è possibile ottenere (sotto forma di report tabellari e/o grafici):
  - Anagrafica e report del parco macchine, rilevate all'interno della rete, organizzate secondo gruppi definiti dagli operatori che utilizzeranno la console;
  - Anagrafica e report degli stati (attivo, allarme, errore, inattivo) per ciascuna macchina sulla quale è installato il software;
  - Anagrafica e report delle versioni del SW e stato dell'aggiornamento.

- **Generazione audit trail e gestione profili di audit**
  La piattaforma è in grado di gestire la generazione di log in modalità nativa sulla piattaforma Windows. Tali log delle attività rilevate sono memorizzate in un registro dedicato all'interno del sistema operativo Microsoft e sono visualizzabili anche tramite la console di gestione. All'interno della console sono configurabili profili di audit per l'accesso a questi log, che possono a loro volta essere memorizzati in un archivio interno.
- Compatibilità con i maggiori protocolli di rete di livello application quali FTP/SFTP/FTPS, HTTP/HTTPS, SMTP e di livello network e transport.
  La piattaforma, lavorando a livello di endpoint, è in grado di intercettare qualsiasi tipo di accesso ai dati o trasmissione degli stessi.
- Compatibilità con i sistemi operativi Windows e Linux
  La piattaforma è compatibile con i sistemi operativi Microsoft Windows. Alcune componenti della console sono anche fruibili su sistema operativo Linux, tra cui, a titolo esemplificativo, la WebGUI per l'accesso tramite web browser alle funzionalità di visualizzazione dei log.

La soluzione è installabile sulle piattaforme seguenti:

Versione desktop:
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10

Versione server:
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Linux (Web GUI).

RaPToR è compatibile con ambienti di tipo Hosted Virtual Desktop.