MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA LOTTA ALLA CONTRAFFAZIONE
UFFICIO ITALIANO BREVETTI E MARCHI

UIBM

DOMANDA DI INVENZIONE NUMERO	**102021000024438**
Data Deposito	**23/09/2021**
Data Pubblicazione	**23/03/2023**

Classifiche IPC

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
G	06	F	21	56

Titolo

SISTEMA DI SICUREZZA INFORMATICA CONTRO MINACCE EVOLVENTI

DESCRIZIONE

a corredo di una Domanda di Brevetto per Invenzione Industriale avente per titolo:

"SISTEMA DI SICUREZZA INFORMATICA CONTRO MINACCE EVOLVENTI"

A nome: Maurizio DE SANTIS

residente in: Str. Mr. Octavian Nita 45 - 550270 SIBIU - Romania

A nome: Jutatip BOONTAWEE

residente in: Via Arturo Toscanini, 40 - 00124 ROMA

con mandatario: Dott.ssa Giuliana CIONCOLONI

La presente invenzione si riferisce ad un sistema di sicurezza informatica contro le minacce quali malware e tentativi di accesso non autorizzati.

Come è noto, è sempre maggiore la complessità delle tecnologie e delle risorse messe in campo per contrastare gli attacchi informatici sferrati ai singoli apparati e ad intere infrastrutture. Tra le ultime tecnologie di contrasto, lo stato della tecnica è rappresentato dallo sviluppo e dall'applicazione di strumenti di Machine Learning (ML) e di *threat intelligence* per il rilevamento di attacchi informatici da parte di malware o di accessi

non autorizzati agli asset sensibili.

Il principale valore aggiunto di queste tecnologie rispetto a quelle tradizionali è rappresentato da una loro capacità adattativa nel processo di individuazione e contrasto rispetto alla continua evoluzione delle minacce.

Va infatti sottolineato che le soluzioni fino ad oggi adottate non consentono di bloccare le minacce "dell'ultima ora" (*zero-day attack*), consentendo, di fatto, una protezione adeguata solo da minacce già censite o da tecniche di intrusione di cui si conosce la tecnica in letteratura.

Il problema non può essere sottovalutato in quanto al numero già esorbitante di minacce censite (oltre 4.000.000 solo facendo riferimento al Kaspersky Lab) si aggiunge la facilità di creazione di nuovi virus resa possibile dalla disponibilità di appositi toolkit che consentono la creazione di sofisticati pattern di attacco anche da parte di sviluppatori non necessariamente "formati" sul tema. Pertanto la protezione dei sistemi informatici è uno dei più importanti compiti di cybersecurity visto che, come si è visto, anche un singolo attacco può determinare una massiva perdita di dati.

La frequenza con cui questi attacchi si verifica,

determina la necessità di una accurata metodologia di rilevamento delle minacce, specialmente rivolta ai cosiddetti "zero-day attacks".

La diversità, la sempre maggiore complessità e il sempre maggior numero di minacce pone una sfida enorme alla ricerca della sicurezza dei sistemi informatici.

Le tecniche tradizionali di analisi, basate sia sull'esame statico che dinamico, presentano dei problemi non del tutto risolti. Non ultimo è l'affacciarsi di nuove generazioni di malware che a loro volta usano tecniche di Machine Learning per portare i loro attacchi.

Per questo si stanno affermando sempre più tecniche basate sull'analisi "comportamentale" del processo da monitorare, per determinare in tempo reale se il processo stesso è un malware o meno.

Per far fronte ai problemi sopra citati e soprattutto per affrontare il problema dei virus non precedentemente classificati (*zero-day attack*), è stato proposto il machine learning (ML) per integrare le soluzioni esistenti.

Il ML si basa su un workflow iterativo che parte dalla raccolta dati, il loro trattamento di bonifica e preparazione, la creazione di uno o più modelli,

la validazione di questi ultimi ed infine la loro messa in produzione.

A seguito dei recenti sviluppi nel campo della visione artificiale, interpretazione del linguaggio naturale ed altri temi avanzati, lo sviluppo di tecniche di Deep Learning è stato proposto anche nel campo della lotta ai malware e ai processi di cybersecurity.

Alcune di queste soluzioni si propongono di addestrare i modelli interamente con i dati che derivano dall'osservazione diretta dei processi con ovvi vantaggi sui tempi di sviluppo in quanto si aggira il problema di ottenere una base di dati aggiornata di firme e dati caratteristici dei malware conosciuti.

L'esigenza attualmente sentita è quella di avere un prodotto capace di rilevare in tempo reale un malware sconosciuto (*zero day attack*) in modo da garantire automaticamente la protezione dell'intero sistema di cybersecurity.

La presente invenzione si pone lo scopo di fornire mezzi per la protezione degli end point e mezzi di Smart Security per la threat intelligence.

Tale scopo è raggiunto fornendo mezzi in grado di eseguire una analisi di un qualsiasi processo

sconosciuto (FUTURE-READY ATTACK PROTECTION) basandosi esclusivamente su pattern comportamentali rilevati nel corso dell'esecuzione stessa.

L'analisi del processo viene eseguita in una modalità "protetta", per cui fino all'esito dell'analisi stessa al processo non è consentita alcuna azione dannosa.

La presente invenzione precettivamente non necessita di un sistema basato su firme o catalogazioni pregresse del processo in esame, e non richiede nemmeno l'esecuzione di un processo sospetto in un ambiente di controllo del tipo sandbox, Virtual Machine o simili.

La determinazione di un'"anomalia comportamentale" viene definita da modelli ricavati da algoritmi di Machine Learning (ML) addestrati su server dedicati. I modelli ottenuti da questo sistema di analisi vengono continuamente aggiornati, redistribuiti e usati dal sistema di monitoraggio installato sugli agent.

Il sistema della presente invenzione consiste in una architettura che prevede una rete di componenti connessi tra loro.

I componenti sono implementati sotto forma di processi fisici distinti, in modo da soddisfare i

criteri di ridondanza, resilienza e sicurezza di tutto il prodotto.

Ogni processo possiede uno status di vitalità definito come MANDATORIO oppure OPZIONALE.

Ogni processo è connesso agli altri tramite comunicazione interprocessi (IPC) su socket e scambia di continuo con gli altri un messaggio di vitalità in modo da informare gli altri processi del proprio stato attivo.

Qualora uno dei processi rilevi che un processo mandatorio non invia più messaggi di vitalità, quest'ultimo viene immediatamente riavviato, in modo da ripristinarne la funzionalità.

Perciò, costituisce oggetto della presente invenzione un sistema secondo l'allegata Rivendicazione 1.

Costituisce anche oggetto della presente invenzione un sistema secondo l'allegata Rivendicazione 2.

Costituisce anche oggetto della presente invenzione un sistema secondo l'allegata Rivendicazione 3.

La presente invenzione sarà compresa in base alla seguente descrizione in riferimento al disegno allegato, in cui l'unica FIGURA 1 illustra

l'architettura del sistema della presente invenzione.

In riferimento alla FIGURA 1 i componenti principali dell'architettura del sistema della presente invenzione sono:

Nome	**Status**	**Collo-cazione**	**Descrizione**
DEVICE DRIVER LAYER (3)	MANDA-TORIO	End point	Consiste in un gruppo di device driver dedicati all'intercettazione a basso livello di una serie di eventi quali: • avvio di processi e threads (5) • I/O Request Packet (IRP) sui file system attivi (7) • Traffico di rete in entrata e in uscita (9) • Eventuali accessi all'MBR (Master Boot Record) (11) • Variazioni anomale dell'utilizzo della

			memoria fisica (13) • Utilizzo del registry (15) Gli eventi vengono rilevati ed inviati tramite IPC al modulo SYSTEM MONITOR (1)
HEALTH SYSTEM (17)	MANDA-TORIO	End point	Unico scopo di questo modulo è la verifica dello stato di vitalità dei processi mandatori. Qualora uno di essi non risulti attivo, HEALTH SYSTEM provvede al riavvio del processo che non risponde. Qualora sia HEALTH SYSTEM a non essere attivo, il compito di riavviare HEALTH SYSTEM spetta a SYSTEM MONITOR. Tramite questo doppio controllo, viene garantita la non interrompibilità dell'intero sistema.
SYSTEM	MANDA-	End	Rappresenta il nodo

MONITOR (1)	TORIO	point	centrale dell'applicazione essendo connesso a tutti gli altri processi tramite IPC. Scopo del modulo è • Ricevere gli eventi rilevati dal DEVICE DRIVER LAYER • Distribuire gli eventi ai processi che sottoscrivono questo tipo di telegrammi e che analizzano gli stessi • Ricevere da GATEWAY aggiornamenti su componenti software, processi in black list, aggiornamenti sui modelli di machine learning • Aggiornare la black list locale in caso sia rilevato un processo

			malevolo • Terminare i processi segnalati come malevoli dai processi dedicati • Gestire la partizione di quarantena e i file in essa contenuti
GATEWAY (19)	MANDA-TORIO	End point	Questo modulo è responsabile delle funzioni di comunicazione e aggiornamento da e per il sistema remoto (HUB Server). Lo scambio di dati in uscita da questo modulo verso l'HUB riguarda i seguenti dati: • Eventi critici quali processi malevoli rilevati • Dump di processi potenzialmente malevoli da far

			esaminare alla struttura centrale • IOC (indicatori di compromissione) rilevati localmente I dati in entrata dall'HUB invece consistono in • Aggiornamenti software (la presenza di aggiornamenti viene notificata al SYSTEM MONITOR che provvede al riavvio dei moduli interessati) • Aggiornamento della black list e degli IOC (indicatori di compromissione) • Aggiornamento dei modelli di machine learning
BEHAVIOR	MANDATORIO	End point	Questo modulo è specializzato

ANALYZER (21)			nell'effettuare una analisi comportamentale dei processi attivi sul sistema allo scopo di individuare eventuali azioni malevole da parte degli stessi. L'analisi comportamentale viene effettuata a partire dagli eventi ricevuti dal processo SYSTEM MONITOR che vengono elaborati da un set dinamico di regole determinato da un modello di machine learning. Vengono analizzati in particolare i seguenti eventi: • Creazione di processi da parte di altri processi • Accessi a chiavi particolari di registry • Utilizzo dei file con particolare riguardo alle

			operazioni in scrittura e al valore entropico differenziale rispetto agli altri processi • Accesso a particolari locazioni fisiche del disco • Creazione e lancio di file eseguibili • Accesso a indirizzi di rete sospetti Nel caso le regole definiscano un processo come anomalo, questo viene segnalato a SYSTEM MONITOR che provvede ad interromperlo e metterlo nella partizione di quarantena.
STATIC ANALYZER (23)	MANDATORIO	End point	Questo processo esegue la classica analisi statica dei processi in esecuzione e dei file eseguibili presenti sul disco (anche

			non in esecuzione). Il modulo esegue anche la scansione preventiva dei file system rimovibili (chiavi usb, HDD esterni, etc), quando questi vengono inseriti. Nel corso dell'analisi Vengono utilizzati gli IOC (indicatori di compromissione) provenienti dall'HUB server e, nel caso un processo venga individuato come anomalo, questo viene segnalato a SYSTEM MONITOR che provvede ad interromperlo e metterlo nella partizione di quarantena
RANDOM FOREST ML ANALYZER (25)	MANDATORIO	End point	Questo processo esegue l'analisi dinamica dei processi in esecuzione utilizzando un modello di machine learning derivato da Random Forest.

			Il modello viene addestrato sul HUB server da procedure dedicate e viene eseguito in recall sull'end point da questo modulo. Nel caso un processo venga individuato come anomalo, questo viene segnalato a SYSTEM MONITOR che provvede ad interromperlo e metterlo nella partizione di quarantena
GUI (27)	OPZIO-NALE	End point	Il modulo è attivo solo su attivazione dell'utente e provvede una dashboard locale per visualizzare lo stato di protezione del dispositivo e le operazioni disponibili, quali visualizzazione status, riavvio, interruzione del servizio di monitoring, scansione del disco.
HUB Server	OPZIO-NALE	Remoto	Questo modulo risiede su infrastruttura Tecninf e

(29)			contiene il database degli eventi e il motore di machine learning dedicato all'analisi degli eventi e gli altri dati provenienti dai vari end point. Di seguito le funzionalità dell'HUB ML service: • Riceve dagli Endpoint AI service (client) i metadati relativi all'esecuzione dei processi e al profilo operativo dell'endpoint • Raccoglie i metadati per creare in modalità non supervisionata profili e classificazioni per tipologia di endpoint e singolo processo (osservazioni comportamentali).

			• Crea e mantiene la base dati con profili, classificazioni e osservazioni comportamentali per singolo processo. • Attiva i processi di machine learning sulle osservazioni comportamentali allo scopo di individuarne i pattern prevedibili e desiderati. • Effettua la modellazione dei pattern e redistribuisce i modelli ottenuti agli Endpoint AI service per l'utilizzo live. • Riceve dagli Endpoint le segnalazioni dei tentativi di attacco

			rilevati tramite anomaly detection salvando dati e metadati utili al team di analisi • Redistribuisce ai client (Endpoint) le informazioni relative a processi classificati benevoli o malevoli in termini di hashcode e metadati (IOC) in modo che questi possano aggiornare le white, black e gray list. • Mantiene una base dati statistica relativa agli attacchi registrati a scopo di monitoraggio.

RIVENDICAZIONI

1. Sistema informatico comprendente in combinazione:
   - un modulo SYSTEM MONITOR (1) rappresentante nodo centrale connesso a tutti gli altri processi del sistema stesso tramite comunicazione interprocessi IPC, ed il quale
   - riceve gli eventi rilevati da un DEVICE DRIVER LAYER (3)
   - distribuire gli eventi ai processi che sottoscrivono questo tipo di telegrammi e che analizzano gli stessi;
   - riceve da un modulo GATEWAY (19) aggiornamenti su componenti software, processi in black list, aggiornamenti sui modelli di machine learning;
   - aggiorna detta black list locale in caso sia rilevato un processo malevolo;
   - termina i processi segnalati come malevoli dai processi dedicati;
   - gestisce la partizione di quarantena e i file in essa contenuti;
   - detto DEVICE DRIVER LAYER (3) comprendendo device driver dedicati all'intercettazione a basso livello di eventi di:

- avvio di processi e threads (5)
- I/O Request Packet (IRP) sui file system attivi (7)
- traffico di rete in entrata e in uscita (9)
- accessi all'MBR (Master Boot Record) (11)
- variazioni anomale dell'utilizzo di memoria fisica (13)
- utilizzo del registry (15);

detti eventi essendo rilevati ed inviati tramite comunicazione interprocessi IPC a detto modulo SYSTEM MONITOR (1);

- un modulo HEALTH SYSTEM (17) che verifica lo stato di vitalità di detti processi mandatori, e, qualora uno di essi non risulti attivo, il modulo HEALTH SYSTEM (17) provvede al riavvio del processo che non risponde; ed il quale qualora non sia attivo, è a sua volta riavviato dal modulo SYSTEM MONITOR; talché è effettuato un doppio controllo, che garantisce la non interrompibilità dell'intero sistema;
- un modulo GATEWAY (19) responsabile delle funzioni di comunicazione e aggiornamento da e per il sistema remoto (HUB Server); lo scambio di dati in uscita da questo modulo

verso l'HUB riguarda i seguenti dati:

- eventi critici, inclusi processi malevoli rilevati
- dump di processi potenzialmente malevoli da far esaminare alla struttura centrale
- IOC (indicatori di compromissione) rilevati localmente
- i dati in entrata dall'HUB invece consistono in:
- aggiornamenti software la presenza dei quali viene notificata a detto modulo SYSTEM MONITOR (1) che provvede al riavvio dei moduli interessati;
- aggiornamento della black list e degli IOC (indicatori di compromissione)
- aggiornamento dei modelli di machine learning;

- un modulo BEHAVIOR ANALYZER (21) il quale effettua una analisi comportamentale dei processi attivi sul sistema allo scopo di individuare eventuali azioni malevole da parte degli stessi;

l'analisi comportamentale essendo effettuata a partire dagli eventi ricevuti da detto modulo SYSTEM MONITOR (1) che vengono elaborati da un set dinamico

di regole determinato da un modello di machine learning, inclusi i seguenti eventi:

- Creazione di processi da parte di altri processi
- Accessi a chiavi particolari di registry
- Utilizzo dei file con particolare riguardo alle operazioni in scrittura e al valore entropico differenziale rispetto agli altri processi
- Accesso a particolari locazioni fisiche del disco
- Creazione e lancio di file eseguibili
- Accesso a indirizzi di rete sospetti;

nel caso che le regole definiscano un processo come anomalo, questo essendo segnalato a detto modulo SYSTEM MONITOR (1) che provvede ad interromperlo e metterlo in una partizione di quarantena;

- un modulo STATIC ANALYZER (23) il quale processo esegue una analisi statica dei processi in esecuzione e dei file eseguibili presenti sul disco (anche non in esecuzione);
- ed il quale esegue una scansione preventiva dei file system rimovibili, incluse chiavi usb, HDD esterni, quando questi vengono

inseriti;

- nel corso dell'analisi essendo utilizzati indicatori di compromissione (IOC) provenienti da detto HUB server e, nel caso un processo venga individuato come anomalo, questo viene segnalato a detto modulo SYSTEM MONITOR (1) che provvede ad interromperlo e metterlo nella partizione di quarantena;

- un modulo RANDOM FOREST ML ANALYZER (25), il quale esegue un'analisi dinamica dei processi in esecuzione utilizzando un modello di machine learning derivato da RANDOM FOREST,

il modello essendo addestrato sul HUB server da procedure dedicate ed essendo eseguito in recall sull'end point da questo modulo stesso (25);

nel caso in cui un processo venga individuato come anomalo, questo essendo segnalato a detto modulo SYSTEM MONITOR (1) che provvede ad interromperlo e metterlo nella partizione di quarantena.

2. Sistema secondo la Rivendicazione 1, ulteriormente comprendente

un modulo GUI (27) attivo solo su attivazione dell'utente e che provvede una dashboard locale per visualizzare lo stato di protezione del dispositivo

e le operazioni disponibili, incluse visualizzazione status, riavvio, interruzione del servizio di monitoring, scansione del disco.

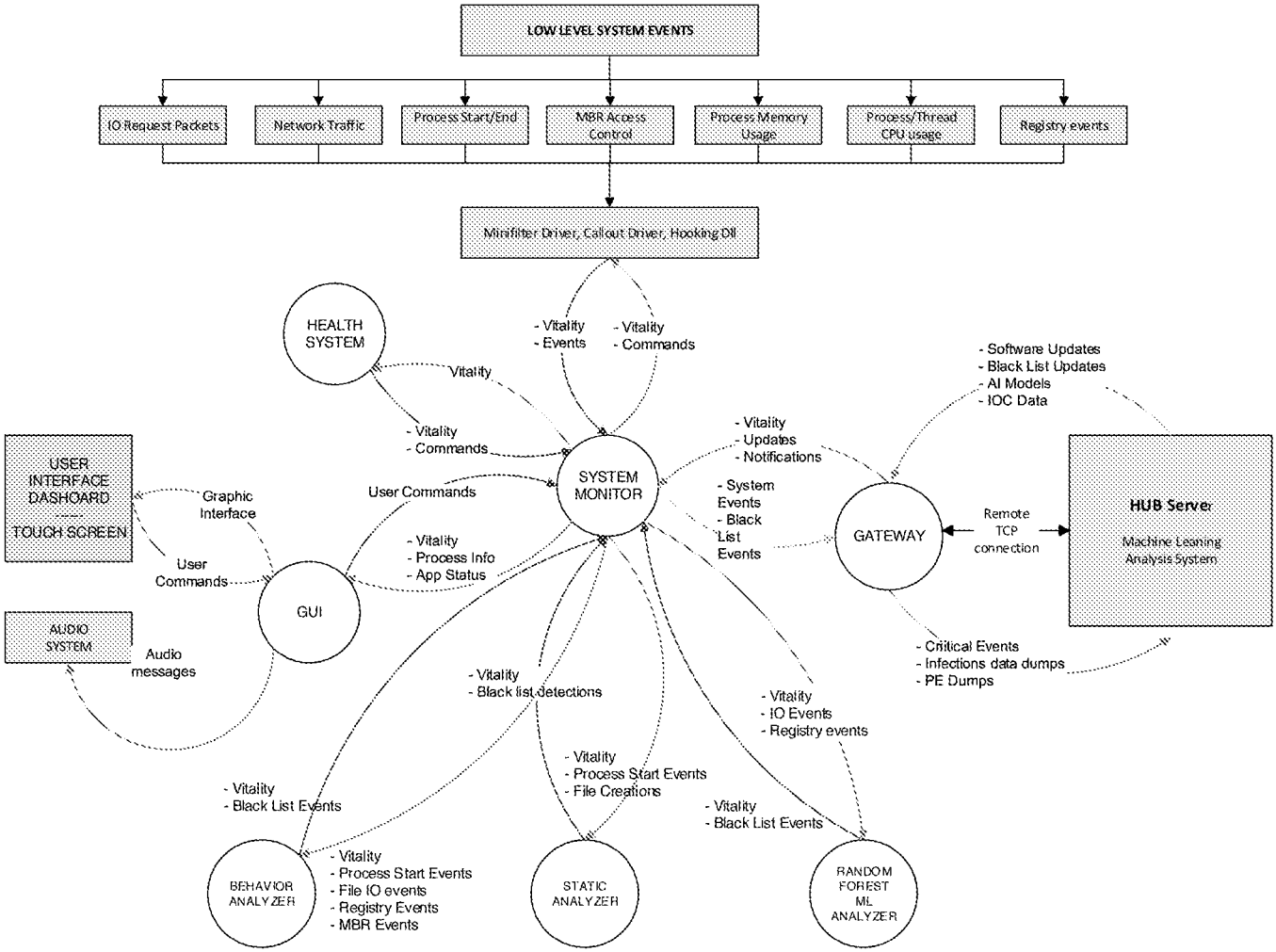
3. Sistema secondo la Rivendicazione 1, ulteriormente comprendente

un modulo HUB Server (29) residente su infrastruttura Tecninf e contenente il database degli eventi e il motore di machine learning dedicato all'analisi degli eventi e gli altri dati provenienti dagli end point, e che

- riceve dagli Endpoint AI service (client) i metadati relativi all'esecuzione dei processi e al profilo operativo dell'endpoint;
- raccoglie i metadati per creare in modalità non supervisionata profili e classificazioni per tipologia di endpoint e singolo processo (osservazioni comportamentali);
- crea e mantiene la base dati con profili, classificazioni e osservazioni comportamentali per singolo processo;
- attiva i processi di machine learning sulle osservazioni comportamentali allo scopo di individuarne i pattern prevedibili e desiderati;

- effettua la modellazione dei pattern e redistribuisce i modelli ottenuti agli Endpoint AI service per l'utilizzo live;
- riceve dagli Endpoint le segnalazioni dei tentativi di attacco rilevati tramite anomaly detection salvando dati e metadati utili al team di analisi;
- redistribuisce ai client (Endpoint) le informazioni relative a processi classificati benevoli o malevoli in termini di hashcode e metadati (IOC) in modo che questi possano aggiornare le white, black e grey list;
- mantiene una base dati statistica relativa agli attacchi registrati a scopo di monitoraggio.

Fig. 1/1


LOW LEVEL SYSTEM EVENTS
IO Request Packets
Network Traffic
Process Start/End
MBR Access Control
Process Memory Usage
Process/Thread CPU usage
Registry events
Minifilter Driver, Callout Driver, Hooking Dll
HEALTH SYSTEM
- Vitality
- Events
- Vitality
- Commands
Vitality
- Vitality
- Commands
SYSTEM MONITOR
- Vitality
- Updates
- Notifications
- Software Updates
- Black List Updates
- AI Models
- IOC Data
USER INTERFACE DASHOARD
TOUCH SCREEN
Graphic Interface
User Commands
User Commands
- Vitality
- Process Info
- App Status
GUI
- System Events
- Black List Events
GATEWAY
Remote TCP connection
HUB Server
Machine Leaning Analysis System
AUDIO SYSTEM
Audio messages
- Critical Events
- Infections data dumps
- PE Dumps
- Vitality
- Black list detections
- Vitality
- IO Events
- Registry events
- Vitality
- Process Start Events
- File Creations
- Vitality
- Black List Events
- Vitality
- Black List Events
BEHAVIOR ANALYZER
- Vitality
- Process Start Events
- File IO events
- Registry Events
- MBR Events
STATIC ANALYZER
RANDOM FOREST ML ANALYZER