

Adrenaline CryptoSentinel	4
Introduzione	5
Architettura del Sistema	6
Interfaccia Utente	7
Descrizione dell'Interfaccia Principale.....	8
Bottone Firewall Rules.....	8
Selezione dell'Interfaccia di Rete	10
Opzioni	11
Elenco parametri "UX_BUFFER":.....	11
Elenco parametri "Options":.....	12
Utilizzo per Rilevare esfiltrazioni di dati tramite protocollo di rete.....	13
Interpretazione dei Dati nel Model Viewer e UX-Buffer	15
Pre-Training	16
Utilizzo delle Opzioni di Configurazione	17
Generazione degli eventi in MS Windows.....	19
Gestione del Time-to-Live (TTL) in AdrenalineFX.....	20
Cos'è il Time-to-Live (TTL)?	20
Importanza del TTL in AdrenalineFX	20
Gestione del TTL in AdrenalineFX.....	20
Modelli Dinamici e Variabilità dei Valori (DFP / DPD)	21
Modelli di Riferimento Dinamici	21
Regolazione del "TimeToLive" del Modello	21
Comportamento dei Valori di DFP e DPD	21
Multi-Score Machine Learning.....	22
Metriche Utilizzate	22
DFD	22
DPD	22
Multi-Score Machine Learning.....	22
Consigli per l'Uso	22
Installazione di Sysmon	23
Download e Installazione di Sysmon.....	23
Scarica Sysmon	23

Estrai il Pacchetto	23
Apri il Prompt dei Comandi come Amministratore	23
Installa Sysmon	24
Crea un file dns.xml	24
Modifica il File di Configurazione XML	24
Disinstallare Sysmon	25
Aggiornare Sysmon	25
Installazione dei Driver PCAP per Windows 10	25
Installazione di NPCAP	25
Scarica NPCAP	25
Esegui l'Installer	25
Avvia il file di installazione	25
Installazione di WIN10PCAP	25
Scarica WIN10PCAP	25
Esegui l'Installer	25
Riavvia il Sistema	26
Installare Adrenaline CryptoSentinel	27
Controllo installazione e verifica	27
Adrenaline RX Engine (Anti-Ransomware).....	29
Introduzione	29
Architettura e Funzionamento di AdrenalineRX.....	29
Entropia del File	29
Byte Magic.....	29
Estensione del File	30
Flusso IO dei File	30
File Canarino	30
Sinergia delle Tecniche di Rilevamento	31
Azioni di Contenimento Estremo	32
Avvio	32
Allarme Sonoro	32
Shut Down Automatico.....	33
File di Configurazione dei Magic Bytes	33

Installazione	33
File di Configurazione (A::RX)	35
Log Level	36
- log0.....	36
- log1.....	36
IO MONITOR.....	38
System Shutdown	39
Monitoring Path	39
File Limiter	39
Valori di soglia	40
Remove Ops.....	40
Max Canary Alarm.....	41
Canary Hide	41
File canary.cfg	41
Escludere i percorsi.....	42
Modifica del File exclude.cfg.....	40
Schema di Versionamento.....	43

Adrenaline CryptoSentinel

Proactive Anti-Data-Exfiltration and reactive Anti-Ransomware.

Versione 1.0 Release Candidate

Requirements : MS Windows 10/11 x64, pcap driver, sysmon64

Tipo di ADX: Multi-Score Machine Learning / Proattivo

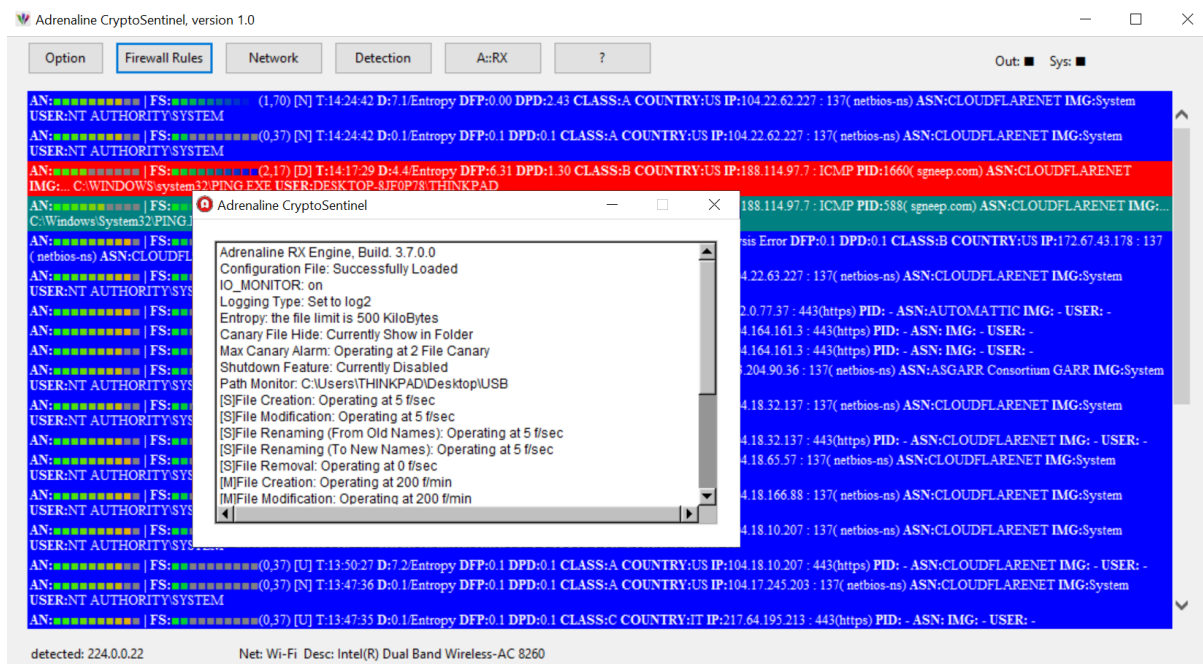
Tipo di Anti-Ransomware: Reattivo

Dissezione Header / Payload: DNS, ICMP, NETBIOS

Layer3 / Layer4

Conversioni: IP to ASN, IP to COUNTRY

Servizi installati: AdrenalineMon5, AdrenalineFX_Service, AdrenalineFX_Firewall



Introduzione

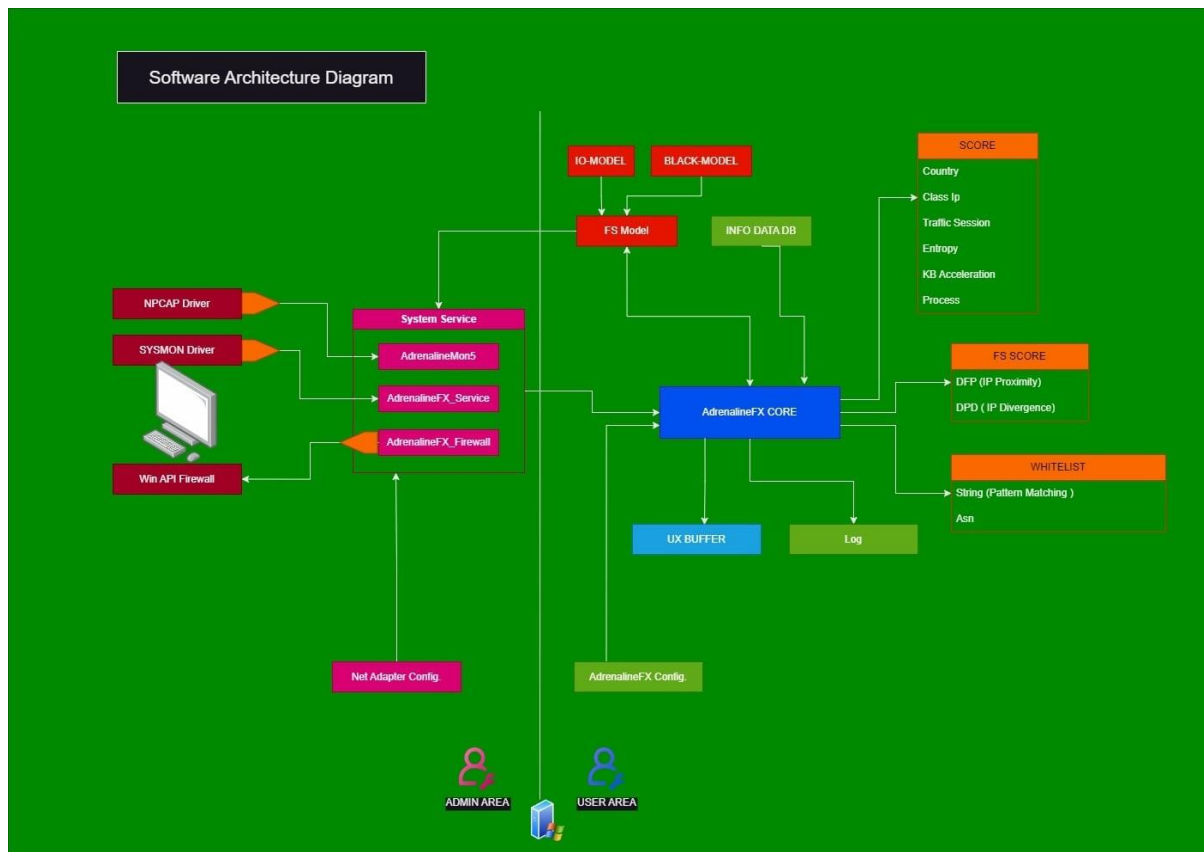
Adrenaline CryptoSentinel è uno strumento progettato con un focus particolare sulla rilevazione e prevenzione dell'esfiltrazione di dati e anti-ransomware.

Questo manuale vi guiderà attraverso le funzionalità principali del software.

Architettura del Sistema

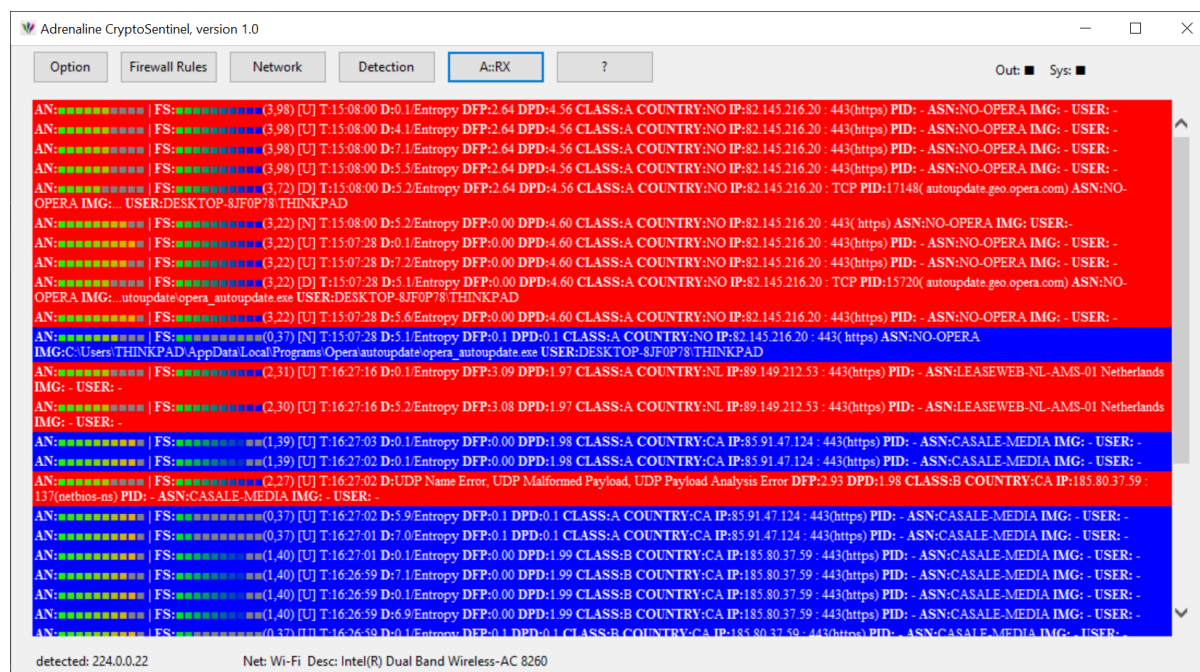
In Adrenaline CryptoSentinel si trovano diversi componenti chiave che lavorano insieme per monitorare e analizzare il traffico di rete. La sua architettura è progettata per garantire un'analisi dettagliata e tempestiva delle attività di rete.

Ver. 0.1



Interfaccia Utente

UX-BUFFER



La schermata principale mostra gli ultimi dati di log (fino a 25 righe) che scorrono dall'alto verso l'alto il basso.

Ogni riga dell'UX-BUFFER fornisce informazioni dettagliate sul traffico di rete:

FS: Flow Score, rappresenta la gravità del flusso di dati. Deve essere abilitato (finestra "opzioni"--> "FS(flow score)" --> "Use")

T: Orario del rilevamento.

D: Entropia del pacchetto, un'indicazione di dati cifrati o compressi.

DPD: Divergenza calcolata dal modello.

DFP: Indicatore di prossimità calcolata dal modello

CLASS: Classe IP.

COUNTRY: Paese di destinazione dell'IP.

IP: Indirizzo IP e porta.

ASN (Sistema autonomo di rete): è numero univoco che viene assegnato alle reti locali dall'American Registry for Internet Numbers (ARIN).

IMG (Immagine del sistema): Indica l'applicazione o servizio che ha inviato i dati.

USER: Il nome utente del sistema in uso.

Descrizione dell'Interfaccia Principale



L'interfaccia principale comprende diverse schede e opzioni per una gestione e monitoraggio ottimale del traffico di rete:

Bottoni

- “Options”
- “Firewall Rules”
- “Network ID”
- “Detections”
- “A::RX”
- “?”

Virtual LEDs: Indicatore che mostra lo stato dei dati in output (Out).

UX-Buffer: Visualizza un log con voci codificate a colori.

Status: La stringa di stato/informazioni.

Bottone apertura regole del Firewall

La finestra “Firewall Rules” permette di gestire le regole del firewall. Adrenaline CryptoSentinel inserisce automaticamente regole per bloccare IP o processi quando viene rilevato uno score di rischio elevato. Da questo pannello è possibile rimuovere la regola dal firewall.

Le regole del firewall sono generate automaticamente da AdrenalineFX per bloccare il traffico sospetto.

AdrenalineFX crea le regole in uscita bloccando l'esfiltrazione a livello di IP o Applicazione.

Firewall Rules				
	Name	Remote Address	Protocol	Application Name
▶	A:FX:188.114.96.7:ip	188.114.96.7	Any	
	A:FX:188.114.97.7:ip	188.114.97.7	Any	
	A:FX:185.235.86.77:ip	185.235.86.77	Any	
	A:FX:85.91.47.142:ip	85.91.47.142	Any	
	A:FX:185.235.86.66:ip	185.235.86.66	Any	
	A:FX:185.235.86.58:ip	185.235.86.58	Any	
	A:FX:89.149.193.117:ip	89.149.193.117	Any	
	A:FX:185.235.86.233:ip	185.235.86.233	Any	
	A:FX:185.235.86.85:ip	185.235.86.85	Any	
	A:FX:185.235.86.82:ip	185.235.86.82	Any	
	A:FX:81.17.55.161:ip	81.17.55.161	Any	
	A:FX:104.18.40.158:ip	104.18.40.158	Any	
	A:FX:192.243.100.216:ip	192.243.100.216	Any	
	A:FX:185.235.86.73:ip	185.235.86.73	Any	

Remove selected rule

Rimozione di una regola: nel pannello seleziona la linea di interesse e premi "Remove selected rule" in basso.

Name: Nome della regola e utente.

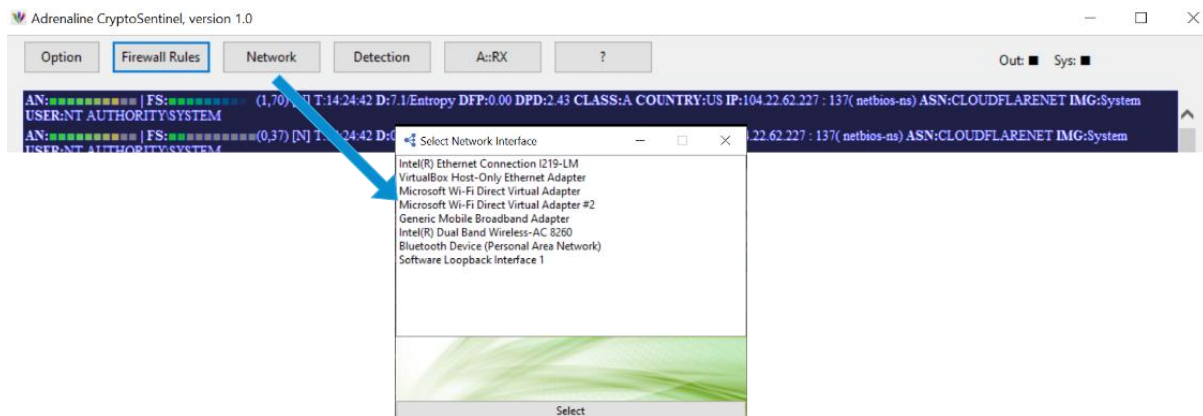
Remote Address: Indirizzo remoto.

Protocol: Protocollo utilizzato (any).

Application Name: Nome dell'applicazione bloccata (nel firewall viene bloccata esclusivamente la connessione in uscita di un dato ip o applicazione.

Bottone selezione dell'Interfaccia di Rete

Il pannello di controllo “Select Network Interface” consente di scegliere l'interfaccia di rete da monitorare.



Attenzione: solo ed esclusivamente con account “amministratore” è possibile cambiare le impostazioni di rete in Adrenaline CryptoSentinel.

Seleziona l'interfaccia appropriata e conferma la scelta con il pulsante “Select”.

(Il pannello di controllo si chiuderà automaticamente e dopo pochi secondi è possibile vedere gli aggiornamenti di stato direttamente nell'interfaccia principale.)

Bottone Opzioni

AdrenalineFX Options

WHITELIST / DATA:

W.List ASN W.List ASN DATA COUNTRY

SCORE WEIGHT :

DNS : 3

ASN : 10

TRAFFIC (KB): 3

IP CLASS: 5

USER : 6

PROCESS : 15

ENTROPY : 5

KB PARTIAL : 10

FX MODEL : 5

ACCELERATION (KB) : 0.70

MODEL :

Time To Live: Day: 0 Hour: 1

DFP (data flow proximity): 1.70

DPD (data pattern divergence): 1.00

FS (flow score): 1.70 ☒ : Use

UX BUFFER:

☐ Show WhiteList

☒ Show Dns

☒ Realtime

OPTIONS:

☒ Use Windows Firewall

☐ Use Event Track

☒ Inherit IP

☐ Lock Pre-Training

Save Default Values

Il pannello opzioni consente di configurare i vari parametri del motore AdrenalineFX.

Elenco parametri "UX_BUFFER":

- Show WhiteList: Abilita la visualizzazione dei pacchetti contrassegnati come leciti. Disabilitare questa opzione per eliminare il rumore nell'output del UX_Buffer.
-
- Show Dns: Abilita la visualizzazione dei log generati da Sysmon con ID 22. Disabilitare questa opzione in produzione.
-
- Realtime UX: Abilita la visualizzazione in tempo reale dei pacchetti. Disabilitare questa opzione in produzione.

NOTA: L'UX Buffer è composto da 25 righe, lavora in tempo reale per ottemperare alle fasi di debug e gestire gli allarmi in tempo reale.

Per una visualizzazione dettagliata è possibile aprire i file di log

Elenco parametri "Options":

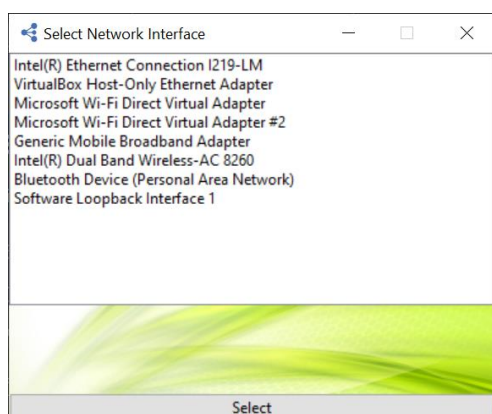
- Use Windows Firewall: abilita la possibilità di generare e inserire regole in "Windows Defender Firewall"
- Inherit IP: abilita l'eredità dell'ip che precedentemente sono stati messi in lista bianca.
- Lock Pre-Training: Abilitando questo flag si blocca il pre-training.
(vedere la parte sul *TRAINING* in questo manuale)

Utilizzo per Rilevare esfiltrazioni di dati tramite protocollo di rete.

Il motore AdrenalineFX integrato in Adrenaline CyberSentinel è progettato per rilevare potenziali esfiltrazioni di dati attraverso un'analisi approfondita del traffico di rete. Ecco alcuni passaggi per utilizzare efficacemente il software:

NOTA: Assicurarsi che il driver npcap (o win10cap) e sysmon sia correttamente installato e funzionante.

Selezione dell'Interfaccia di Rete: Utilizzare la scheda "Network" per selezionare l'interfaccia di rete:

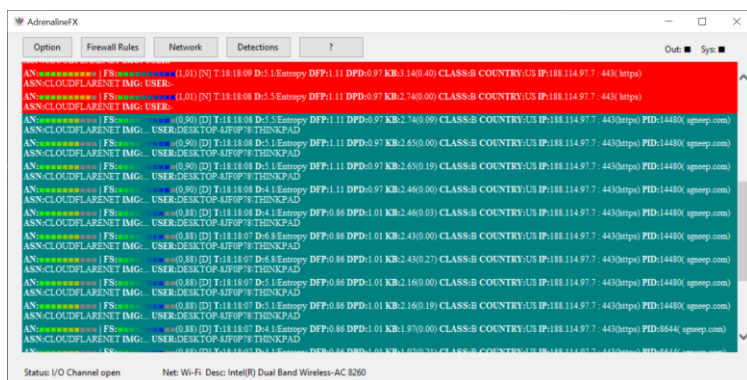


Visualizzazione dei rilevamenti a cui è stato disabilitato l'accesso: Nella scheda "Detections", monitorare le voci di log per informazioni appartenenti all'IP, nella scheda "Firewall Rules" vedere gli ip contrassegnati come bloccati.

Interpretazione dei Dati nel Model Viewer e UX-Buffer

- AN (Anomaly Score): Indica il rischio associato a un flusso di dati.(experimental)
- FS (Flow Score): Rappresenta la gravità del flusso di dati.
- ENTROPIA: Identifica dati cifrati o compressi,
- DPD (Data Pattern Divergence): Misura la deviazione dal comportamento in un arco temporale definito.
- DFP (Data Flow Proximity): Indica la prossimità su di un modello di ip noto in un arco temporale definito

Nella figura sotto il valore di soglia FS è impostato ad 1.0 ,regolare questo valore secondo le preferenze nel pannello “Option” alla voce “FS (flow score)”.



Puoi regolare i parametri DFP e DPD anche singolarmente, in FS(flow score) disabilita il checkbox “Use”.

Pre-Training

Nel Pre-Training vengono sfruttati i dati Sysmon e vengono incrociati con i dati inseriti nella whitelist (W.List), la W.List accetta qualsiasi stringa confrontabili con le stringhe che appaiono nel UX-Buffer e Log.

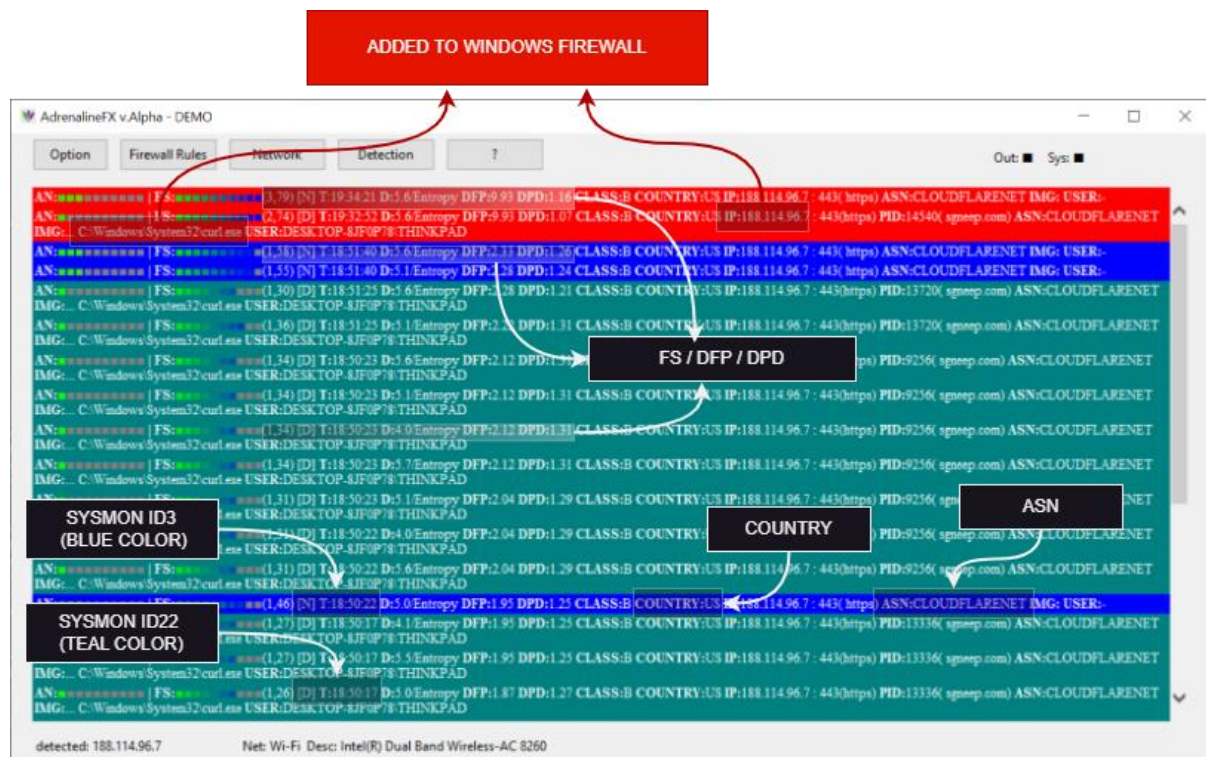
Una volta effettuato il pre-training (generalmente pochi secondi) e possibile bloccarlo con il radioButton Lock Pre-Training nel pannello opzioni di Adrenaline CryptoSentinel.

Uso del pre-training:

Il pre-training parte all'avvio di Adrenaline CryptoSentinel, puoi bloccare il pre-training quando vuoi, questo crea una finestra di addestramento per escludere il rumore generato dall'uso lecito.

Nota: Il pre-training può essere disattivato togliendo la spunta alla voce "inherit IP".

Utilizzo delle Opzioni di Configurazione



Accesso al Menu Opzioni: Configurare le opzioni per adattare il software alle esigenze specifiche.

Configurazione del TimeToLive: Nel pannello di controllo, è possibile impostare la durata di vita del modello. Questo parametro determina per quanto tempo un modello rimane attivo prima di essere rigenerato, influenzando la frequenza degli aggiornamenti e la sensibilità del sistema.

Configurazione di DPD e DFP: Questi parametri vengono utilizzati per monitorare e analizzare il traffico di rete. DPD (Data Pattern Divergence) e DFP (Data Flow Proximity) si adattano dinamicamente al traffico di rete, aggiornando i modelli di riferimento per riflettere le condizioni attuali.

Calcolo dello Score (FS): Il parametro FS (Flow Score) rappresenta il risultato combinato delle analisi di DFP e DPD. Questo score fornisce una valutazione

complessiva della sicurezza del traffico di rete, aiutando a identificare potenziali minacce.

Generazione degli eventi in MS Windows

The screenshot displays the Windows Event Viewer and the Adrenaline CryptoSentinel application. The Event Viewer shows a list of events from the 'AdrenalineFX_FirewallService' application. The details pane shows an event titled 'Added application in MS firewall rule 'A:FX:188.114.97.7_app_THINKPAD''. Below this, a green box highlights the text 'outgoing connection blocked' and another green box highlights 'Application Level / User'. The Adrenaline CryptoSentinel application is open, showing the 'Firewall Rules' tab. The logs show various network events, including a ping request from 'C:\WINDOWS\system32\PING EXE' to 'USER-DESKTOP-SJFUP78-THINKPAD'.

Visualizzatore eventi

File Azione Visualizza ?

Visualizzatore eventi (computer)

Visualizzazioni personalizzate

Registri di Windows

Applicazione

Sicurezza

Installazione

Sistema

Eventi inoltrati

Registri applicazioni e servizi

Sottoscrizioni

Applicazione Numero di eventi: 72.712

Livello	Data e ora	Origine	ID evento	Categoria attività
Informazioni	30/09/2024 14:17:30	AdrenalineFX_FirewallSe...	0	Nessuna
Informazioni	30/09/2024 14:17:30	AdrenalineFX_FirewallSe...	0	Nessuna
Informazioni	30/09/2024 12:44:06	Security-SPP	16384	Nessuna
Informazioni	30/09/2024 12:43:28	Security-SPP	16394	Nessuna
Informazioni	30/09/2024 12:43:20	ESENT	326	Generale
Informazioni	30/09/2024 12:43:20	ESENT	106	Generale

Evento 0, AdrenalineFX_FirewallService

Generale Dettagli

Added application in MS firewall rule 'A:FX:188.114.97.7_app_THINKPAD'

outgoing connection blocked

Application Level / User

Adrenaline CryptoSentinel, versione 0.0

Option Firewall Rules Network Detection A:RX ?

Out: Sys

AN: [FS: (1,70) [N] T:14:24:42 D:7.1 Entropy DFP:0.00 DPD:2.43 CLASS:A COUNTRY:US IP:104.22.62.227 : 137(netbios-ns) ASN:CLOUDFLARENET IMG:System USER:NT AUTHORITY\SYSTEM

AN: [FS: (0,37) [N] T:14:24:42 D:0.1 Entropy DFP:0.1 DPD:0.1 CLASS:A COUNTRY:US IP:104.22.62.227 : 137(netbios-ns) ASN:CLOUDFLARENET IMG:System USER:NT AUTHORITY\SYSTEM

AN: [FS: (0,12) [D] T:14:17:29 D:4.4 Entropy DFP:6.31 DPD:1.30 CLASS:B COUNTRY:US IP:188.114.97.7 : ICMP PID:1660(sgneep.com) ASN:CLOUDFLARENET IMG: C:\WINDOWS\system32\PING EXE USER:DESKTOP-SJFUP78-THINKPAD

AN: [FS: (1,06) [D] T:14:17:22 D:4.4 Entropy DFP:1.06 DPD:1.21 CLASS:B COUNTRY:US IP:188.114.97.7 : ICMP PID:388(sgneep.com) ASN:CLOUDFLARENET IMG: C:\WINDOWS\system32\PING EXE USER:DESKTOP-SJFUP78-THINKPAD

AN: [FS: (0,37) [N] T:14:01:25 D:0.1 UDP Name Error, UDP Malformed Payload, UDP Payload Analysis Error DFP:0.1 DPD:0.1 CLASS:B COUNTRY:US IP:172.67.43.178 : 137(netbios-ns) ASN:CLOUDFLARENET IMG:System USER:NT AUTHORITY\SYSTEM

AN: [FS: (0,37) [N] T:13:37:16 D:6.7 Entropy DFP:0.1 DPD:0.1 CLASS:A COUNTRY:US IP:104.22.62.227 : 137(netbios-ns) ASN:CLOUDFLARENET IMG:System USER:NT AUTHORITY\SYSTEM

AN: [FS: (0,37) [N] T:13:37:16 D:6.7 Entropy DFP:0.1 DPD:0.1 CLASS:A COUNTRY:US IP:104.22.62.227 : 137(netbios-ns) ASN:CLOUDFLARENET IMG:System USER:NT AUTHORITY\SYSTEM

Azioni

Apri registro salvato...

Crea visualizzazione personali...

Importa visualizzazione perso...

Cancella registro...

Filtro registro corrente...

Proprietà

Trova...

Salva tutti gli eventi con nome...

Associa un'attività al registro...

Visualizza

Aggiorna

Guida

Evento 0, AdrenalineFX_FirewallSer...

Proprietà evento

Associa attività all'evento...

Copia

Salva eventi selezionati...

Aggiorna

Guida

Gestione del Time-to-Live (TTL) in AdrenalineFX

Il Time-to-Live (TTL) del modello di apprendimento è un parametro fondamentale nel monitoraggio del traffico di rete e nella rilevazione delle esfiltrazioni di dati in tempo reale. In AdrenalineFX, il Time-To-Live viene utilizzato per garantire che l'analisi del traffico sia sempre aggiornata e rilevante. Questo capitolo spiega l'importanza del TTL e come viene gestito all'interno del sistema.

Cos'è il Time-to-Live (TTL)?

Il TTL è un valore che indica la durata di vita di un pacchetto di dati in una rete. Ogni pacchetto ha un TTL che viene decrementato di uno ogni volta che attraversa un router. Quando il TTL raggiunge zero, il pacchetto viene scartato. Questo meccanismo impedisce che i pacchetti rimangano indefinitamente in circolazione nella rete.

Importanza del TTL in AdrenalineFX

In AdrenalineFX, il TTL è utilizzato per mantenere l'analisi del traffico di rete focalizzata sui dati più recenti e rilevanti. Ecco perché il TTL è cruciale:

Rimozione dei Dati Obsoleti: Il TTL aiuta a eliminare i pacchetti di dati che hanno superato la loro utilità, garantendo che l'analisi si concentri solo sui pacchetti attuali.

Prevenzione dei Falsi Positivi: Monitorare pacchetti con TTL scaduto può portare a falsi positivi. Utilizzando il TTL, AdrenalineFX riduce il rischio di segnalare attività sospette basate su dati non più rilevanti.

Aggiornamento Continuo: Il TTL assicura che il sistema sia costantemente aggiornato, migliorando la precisione e l'efficacia del rilevamento delle anomalie.

Gestione del TTL in AdrenalineFX

Quando il TTL di un pacchetto scade, AdrenalineFX esegue un "refresh" del modello di analisi. Questo processo garantisce che solo i pacchetti con un TTL valido siano considerati nell'analisi, mantenendo il sistema agile e reattivo.

Modelli Dinamici e Variabilità dei Valori (DFP / DPD)

Modelli di Riferimento Dinamici

In Adrenaline CryptoSentinel e nello specifico nel motore AdrenalineFX, i modelli di traffico fungono da benchmark per valutare l'attività corrente sulla rete. Questi modelli, denominati "Modelli di Riferimento Dinamici", vengono costantemente aggiornati e sostituiti a intervalli regolari definiti dall'utente. Questo processo garantisce che l'analisi sia sempre basata su dati pertinenti e recenti, migliorando l'accuratezza del rilevamento delle anomalie.

Regolazione del "TimeToLive" del Modello

La durata di vita del modello, configurabile dall'utente, determina per quanto tempo un modello rimane attivo prima di essere rigenerato. La scelta del "TimeToLive" (TTL) influisce direttamente sul comportamento dei parametri DFP e DPD.

Comportamento dei Valori di DFP e DPD

I valori di DFP e DPD possono variare in risposta al traffico di rete (in uscita), in base a quanto questo traffico diverge dai modelli attuali. L'algoritmo adatta dinamicamente questi valori per riflettere l'aderenza o la deviazione rispetto ai modelli, facendo sì che la soglia di allarme possa variare in base all'analisi continua del traffico.

- **Aumento dei Valori:** Quando il traffico di rete diverge significativamente dai modelli di riferimento, i valori di DFP e DPD aumentano, indicando una potenziale anomalia.
- **Diminuzione dei Valori:** Se il traffico di rete rientra nei parametri previsti dai modelli, i valori di DFP e DPD diminuiscono, segnalando un comportamento normale.

Multi-Score Machine Learning

Il modulo AdrenalineFX utilizza un approccio avanzato di machine learning chiamato “Multi-Score Machine Learning” per rilevare e prevenire l’esfiltrazione dei dati. Questo metodo si basa sull’uso di più metriche per valutare e analizzare il traffico di rete, garantendo un rilevamento accurato e tempestivo delle anomalie.

Metriche Utilizzate

DFD:

- **Descrizione:** Utilizza la distanza euclidea per misurare la dissimilarità tra i pacchetti di dati. Questa metrica è particolarmente utile per identificare pacchetti che si discostano significativamente dal comportamento normale.

DPD:

- **Descrizione:** Misura la prossimità dei pacchetti di dati rispetto ai modelli di riferimento dinamici. Questa metrica aiuta a rilevare deviazioni sottili e gradualmente nel traffico di rete.

Multi-Score Machine Learning

- **Precisione:** L’uso di più metriche consente di ottenere una visione più completa e accurata del traffico di rete, riducendo il rischio di falsi positivi.
- **Adattabilità:** I modelli di riferimento dinamici vengono costantemente aggiornati, permettendo al sistema di adattarsi rapidamente alle nuove condizioni di rete.
- **Rilevamento Tempestivo:** La combinazione di DPD e DFP permette di rilevare sia anomalie evidenti che sottili, migliorando la capacità di prevenire esfiltrazioni di dati.

La gestione dinamica dei modelli di riferimento e la regolazione del TimeToLive (TTL) sono fondamentali per mantenere l’efficacia del monitoraggio del traffico di rete in AdrenalineFX. Configurando correttamente questi parametri, gli utenti possono ottimizzare il sistema per adattarsi alle specifiche esigenze del loro ambiente di rete, migliorando la precisione del rilevamento delle anomalie e riducendo i falsi positivi.

Consigli per l’Uso

La configurazione ottimale del “TimeToLive” del modello dipende dalle esigenze specifiche dell’utente. In ambienti dove il traffico è soggetto a rapide variazioni, un “TimeToLive” più breve può ridurre i falsi positivi e migliorare la reattività del sistema. In contesti aziendali più stabili, un “TimeToLive” esteso fornisce una visione più robusta e coerente, ideale per identificare attività anomale che si sviluppano lentamente.

L’utente dovrebbe scegliere il “TimeToLive” in base al comportamento tipico del traffico della propria rete, bilanciando la sensibilità agli allarmi e la necessità di adattabilità nel monitoraggio delle potenziali esfiltrazioni di dati.

AdrenalineFX è uno strumento avanzato per la prevenzione dell’esfiltrazione di dati, fornendo gli strumenti necessari per monitorare, analizzare e reagire a potenziali minacce di sicurezza. Con una configurazione appropriata e un’analisi attenta, è possibile proteggere efficacemente la rete da tentativi di esfiltrazione di dati.

Installazione di Sysmon

Sysmon è uno strumento di monitoraggio avanzato per Windows, parte della suite Sysinternals, che fornisce informazioni dettagliate sui processi di sistema, i network connections e altre attività sospette.

Download e Installazione di Sysmon

Scarica Sysmon:

Visita il sito di Sysinternals.

Clicca sul link per scaricare il pacchetto Sysmon.

Estrai il Pacchetto:

Dopo aver scaricato il file ZIP, estrailo in una cartella temporanea a tua scelta e poi sposta il contenuto nella cartella: C:\Sysinternals\Sysmon\

Apri il Prompt dei Comandi come Amministratore:

Cerca "cmd" o "prompt dei comandi" nel menu Start, clicca con il tasto destro e seleziona "Esegui come amministratore".

Installa Sysmon:

Naviga nella cartella in cui hai estratto Sysmon (C:\Sysinternals\Sysmon\) utilizzando il comando cd.

Crea un file dns.xml vuoto e copia il contenuto di questo snippet:

```
<Sysmon schemaversion="4.90">  
  <EventFiltering>  
    <DnsQuery onmatch="exclude"/>  
    <NetworkConnect onmatch="exclude"/>  
  </EventFiltering>  
</Sysmon>
```

Qui dns.xml è il file di configurazione che definisce quali eventi Sysmon deve monitorare. Assicurati di avere questo file nella stessa cartella di Sysmon o specifica il percorso corretto.

Esegui il comando per installare Sysmon:

```
Sysmon64.exe -accepteula -i dns.xml
```

Modifica il File di Configurazione XML

Sysmon usa un file XML per configurare quali eventi raccogliere. Puoi creare o modificare questo file XML secondo le tue esigenze di monitoraggio.

Aggiorna la Configurazione:

```
sysmon -c sysmonconfig.xml
```

Questo aggiornerà la configurazione esistente senza reinstallare Sysmon.

Disinstallazione e Aggiornamento di Sysmon

Disinstallare Sysmon:

Per disinstallare Sysmon, usa il comando:

`sysmon -u`

Aggiornare Sysmon:

Se è necessario aggiornare Sysmon, prima disinstalla la versione esistente e poi segui nuovamente i passaggi di installazione con la nuova versione scaricata.

Installazione dei Driver PCAP per Windows 10

NPCAP e WIN10PCAP sono driver necessari per catturare pacchetti di rete su Windows 10.

Scegli uno dei due, in base alle tue preferenze.

Installazione di NPCAP

Scarica NPCAP: [Npcap: Windows Packet Capture Library & Driver](#)

Esegui l'Installer:

Avvia il file di installazione scaricato e segui le istruzioni sullo schermo.

Installazione di WIN10PCAP

Scarica WIN10PCAP:

Vai al sito di Win10Pcap e scarica l'installer: [Win10Pcap - WinPcap for Windows 10](#)

Esegui l'Installer:

Avvia il file di installazione e segui le istruzioni fornite.

Riavvia il Sistema:

Riavvia il computer per completare l'installazione (se richiesto).

Installare Adrenaline CryptoSentinel

- 1- Scarica AdrenalineFX CryptoSentinel dalla pagina GitHub:
- 2- Esegui AdrenalineCryptoSentinel.exe, al termine dell'installazione puoi avviare AdrenalineFX CyberSentinel con privilegi elevati per poter scegliere la rete di monitoraggio.

Attenzione: Solo gli utenti con privilegi elevati (amministratori) possono modificare le impostazioni di rete.

Controllo installazione e verifica

Le seguenti operazioni richiedono privilegi elevati(admin)

- 1- Assicurarsi di avere installato Net4.8.1 / Net 8.x:
 - Download Runtime 4.8.1: [Download .NET Framework 4.8.1 | Free official downloads \(microsoft.com\)](#)
 - Download Desktop Runtime 8.x: [Download .NET 8.0 \(Linux, macOS, and Windows\) \(microsoft.com\)](#)
- 2- Assicurarsi di avere installato NPCAP o WIN10PCAP
- 3- Assicurarsi di avere scelto l'adattatore di rete corretto nell'apposito menù in AdrenalineFX
- 4- Controllare che i servizi AdrenalineFX_firewall e AdrenalineFX_Service siano avviati
- 5- Leggere il log Windows Event Viewer
- 6- Leggere il file AdrenalineFXMonitorServiceLog.log

Adrenaline RX Engine (Anti-Ransomware)

Approccio Avanzato al Rilevamento dei Ransomware

Introduzione

La proliferazione dei ransomware rappresenta una delle minacce più gravi per la sicurezza informatica contemporanea. I ransomware criptano i dati delle vittime, richiedendo un riscatto per la loro decriptazione. Le tradizionali misure di sicurezza, come antivirus e firewall, spesso non sono sufficienti a contrastare queste minacce in continua evoluzione. Questo studio si concentra su AdrenalineRX, un anti-ransomware sviluppato in C++, che adotta un approccio innovativo basato su una combinazione di tecniche di analisi avanzata per rilevare e prevenire gli attacchi ransomware.

Architettura e Funzionamento di AdrenalineRX

AdrenalineRX utilizza un Sistema di Analisi Avanzata, che esamina ogni file creato nel sistema attraverso cinque principali parametri tecnici: entropia del file, byte magic, estensione del file, flusso IO dei file e gestione dei file canarino.

Entropia del File

L'entropia di un file è una misura del disordine o della casualità nei dati contenuti nel file stesso. In generale, un file criptato presenta un'entropia significativamente più alta rispetto a un file non criptato. AdrenalineRX calcola l'entropia di ogni file per identificare potenziali attività di criptazione. Se l'entropia supera una soglia predefinita, il file viene contrassegnato come sospetto.

Byte Magic

Il termine "byte magic" si riferisce alla presenza di sequenze di byte caratteristiche all'inizio dei file che identificano il tipo di file. Queste sequenze, note anche come "magic numbers", sono utilizzate da AdrenalineRX per verificare la coerenza tra il

contenuto del file e la sua estensione dichiarata. Incongruenze in questo parametro possono indicare un tentativo di nascondere la vera natura di un file maligno.

Estensione del File

Le estensioni dei file sono spesso modificate dai ransomware per nascondere i file criptati o per eseguire script malevoli. AdrenalineRX monitora le modifiche alle estensioni dei file, cercando cambiamenti sospetti che potrebbero indicare un attacco in corso. Questo parametro permette di rilevare rapidamente l'inizio di un'azione malevola prima che possa diffondersi ulteriormente.

Flusso IO dei File

AdrenalineRX analizza in tempo reale le operazioni di input/output dei file nel filesystem, concentrandosi sulle operazioni di creazione, modifica, rinomina ed eliminazione. Un aumento anomalo in queste attività può essere indicativo di un ransomware che sta criptando file. La combinazione di queste informazioni fornisce un quadro dettagliato del comportamento dei file, permettendo di rilevare e bloccare le attività sospette tempestivamente.

File Canarino

AdrenalineRX utilizza anche file canarino come metodo di rilevamento. I file canarino sono file appositamente creati e monitorati che non dovrebbero mai essere modificati durante il normale utilizzo del sistema. Qualsiasi tentativo di accesso, modifica o eliminazione di questi file attiva immediatamente un allarme. Questa tecnica permette di rilevare tentativi di criptazione prima che possano causare danni estesi.

Sinergia delle Tecniche di Rilevamento

La vera forza di AdrenalineRX risiede nella combinazione sinergica di questi parametri. Ogni tecnica fornisce un pezzo del puzzle, e insieme formano un sistema di rilevamento altamente efficace. Ad esempio, un file con elevata entropia ma con un byte magic e un'estensione corretta potrebbe non essere immediatamente sospetto. Tuttavia, se questo file è coinvolto in operazioni di I/O anomale o semplicemente sono stati modificati i file canarino, AdrenalineRX può identificarlo come una potenziale minaccia.

L'approccio multi-parametrico permette di ridurre i falsi positivi e aumentare la precisione del rilevamento. AdrenalineRX non solo identifica i file sospetti, ma anche il comportamento complessivo del sistema, permettendo una risposta tempestiva e mirata alle minacce.

Azioni di Contenimento Estremo

AdrenalineRX è progettato come ultima linea di difesa contro gli attacchi ransomware. Nel caso in cui un attacco riesca a superare le misure di rilevamento iniziali e inizi a criptare i file, AdrenalineRX è in grado di eseguire azioni di contenimento estremo. Tra queste, la più drastica è lo spegnimento immediato del sistema. Spegnerne il sistema può interrompere il processo di criptazione, riducendo i danni ai file non ancora compromessi. Questa funzione è particolarmente utile quando tutte le altre misure di difesa sono fallite.

Avvio

Dopo essere stato avviato, AdrenalineRX visualizza una serie di dati iniziali cruciali per comprendere lo stato del programma e la sua configurazione attuale. Questi dati forniscono informazioni dettagliate sulle impostazioni e le funzionalità attive, tra cui il tipo di log utilizzato, lo stato della funzione di spegnimento, il percorso di monitoraggio dei file e le impostazioni di allarme per le operazioni di creazione, modifica, rinominazione e rimozione dei file.

Allarme Sonoro

Quando AdrenalineRX rileva un'attività sospetta o potenzialmente dannosa, attiva un allarme sonoro per avvisare prontamente l'utente dell'attività anomala in corso. L'allarme sonoro è progettato per catturare immediatamente l'attenzione dell'utente e segnalare la presenza di un potenziale rischio per la sicurezza del sistema.

Il file "ALARM.wav", presente nella cartella radice di AdrenalineRX, contiene il suono dell'allarme utilizzato per questo scopo specifico. Questo file audio è progettato per essere facilmente riconoscibile e distintivo, garantendo che l'utente possa identificare rapidamente l'avviso di una potenziale minaccia.

Gli allarmi sonori svolgono un ruolo fondamentale nelle fasi di analisi e di test prima che AdrenalineRX entri in produzione effettiva. Durante questa fase, gli sviluppatori e gli analisti di sicurezza utilizzano gli allarmi sonori per verificare l'efficacia del sistema nel rilevare e segnalare attività sospette. Questo processo consente di valutare l'affidabilità del sistema e di apportare eventuali ottimizzazioni o miglioramenti necessari prima che AdrenalineRX venga distribuito in un ambiente di produzione.

Shut Down Automatico

Quando AdrenalineRX individua un'attività dannosa, può avviare automaticamente la funzione di spegnimento del sistema per prevenire ulteriori danni e salvaguardare l'integrità dei dati. Questa funzionalità di spegnimento automatico è progettata per intervenire prontamente in situazioni critiche, proteggendo il sistema e i dati dall'espansione dei danni causati da attività malevole.

File di Configurazione dei Magic Bytes (**magic.cfg**)

Nel file di configurazione, ogni riga specifica un tipo di file con la relativa estensione e il corrispondente "Magic Byte" utilizzato per identificare il tipo di file. I magic bytes sono sequenze di byte uniche che si trovano all'inizio di un file e sono utilizzate per determinare il suo tipo o formato. Questi valori vengono poi utilizzati da Adrenaline per riconoscere e gestire correttamente i diversi tipi di file durante le analisi e le operazioni di protezione.

Installazione

Per configurare l'anti-ransomware, segui attentamente questi passaggi:

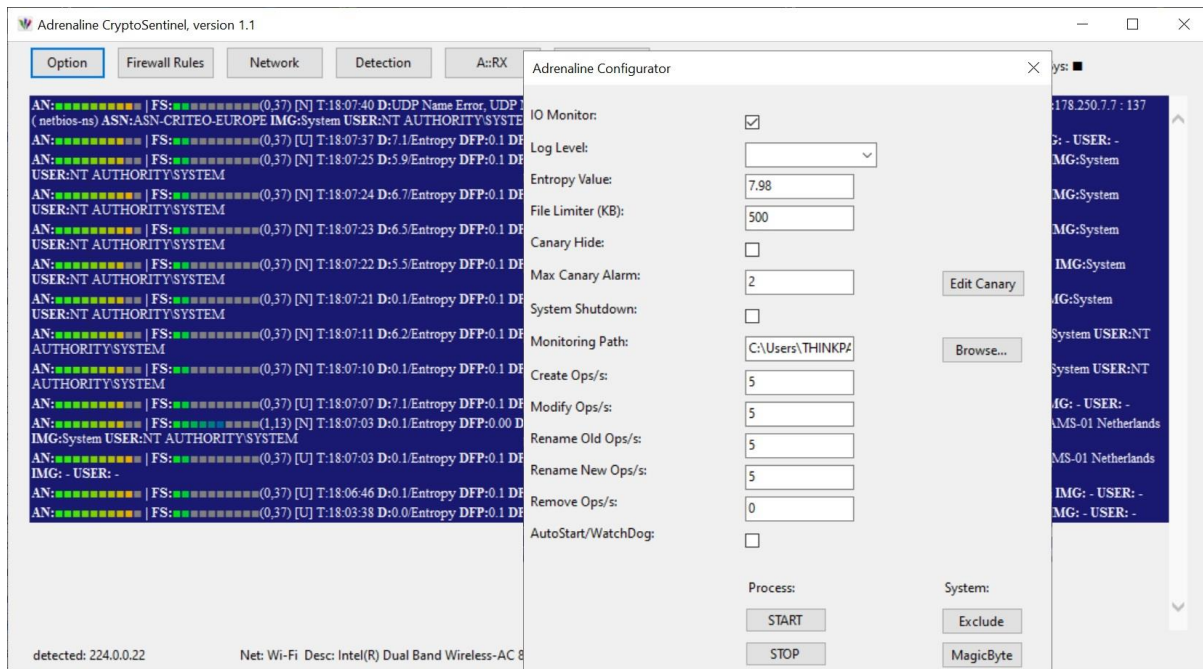
- 1- **Avvia Adrenaline Rx:** Dopo aver installato il programma, avvialo facendo doppio clic sull'icona dell'applicazione.????
- 2- **Configurazione iniziale:** lanciare il modulo Adrenaline Anti-Ransomware, il primo avvio avviene con i valori de default.
Il motore AdrenalineRX Inizierà a monitorare la directory predefinita:
C:/Users/**utente**/Desktop.

- 3- **Apri il file di configurazione:** Per personalizzare le impostazioni, premi il pulsante "A::RX" dall'interfaccia di Adrenaline CyberSentinel. Questo ti permetterà di accedere al file di configurazione dell'anti-ransomware.
- 4- **Modifica le impostazioni.**
- 5- **Salva.**
- 6- **Riavvia Adrenaline Rx:** Per applicare le modifiche, chiudi e riavvia AdrenalineRX. In questo modo, il programma utilizzerà le nuove impostazioni configurate nel file config.cfg.

Seguendo questi passaggi, potrai personalizzare le impostazioni di Adrenaline RX e configurare il programma per adattarlo alle tue esigenze specifiche.

Configurazione Anti-Ransomware (A::RX)

Apri il pannello di controllo “A::FX”



Pannello di configurazione di A:RX

The screenshot shows the 'A:RX Configurator' window with the following settings:

- IO Monitor:** ☒
- Log Level:** (dropdown menu)
- Shannon Value:**
- File Limiter (KB):**
- Canary Hide:** ☐
- Max Canary Alarm:**
- System Shutdown:** ☐
- Monitoring Path:** (with a 'Browse...' button)
- Create Ops/sm:** (left) and (right)
- Modify Ops/sm:** (left) and (right)
- Rename Old Ops/sm:** (left) and (right)
- Rename New Ops/sm:** (left) and (right)
- Remove Ops/sm:** (left) and (right)
- AutoStart/WatchDog:** ☐
- Process:** and
- System:** and
- Buttons:**

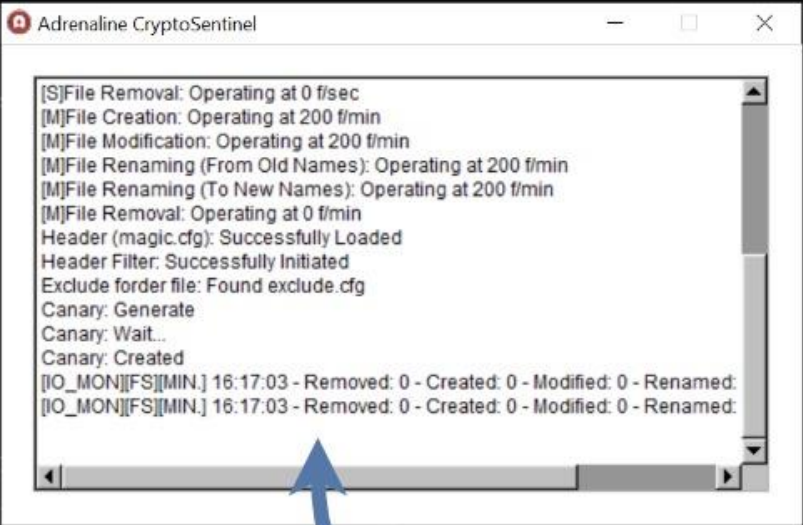
Log Level = <log0 | log1>

Il file di log, essenziale per il tracciamento delle attività, viene generato quotidianamente e può essere trovato nella directory principale di Adrenaline, specificamente nella cartella ".\log".

- **log0:** Questa modalità di registrazione è inattiva, Adrenaline non registra alcun evento.
- **log1:** Abilita questa modalità per visualizzare i file processati da AdrenalineRX.

Solo gli eventi che generano allarmi vengono conteggiati.

Usare log1 solo per attività di verifica.



Adrenaline CryptoSentinel

LOG1

```
[S]File Removal: Operating at 0 f/sec  
[M]File Creation: Operating at 200 f/min  
[M]File Modification: Operating at 200 f/min  
[M]File Renaming (From Old Names): Operating at 200 f/min  
[M]File Renaming (To New Names): Operating at 200 f/min  
[M]File Removal: Operating at 0 f/min  
Header (magic.cfg): Successfully Loaded  
Header Filter: Successfully Initiated  
Exclude folder file: Found exclude.cfg  
Canary: Generate  
Canary: Wait...  
Canary: Created  
[IO_MON][FS][MIN.] 16:17:03 - Removed: 0 - Created: 0 - Modified: 0 - Renamed:  
[IO_MON][FS][MIN.] 16:17:03 - Removed: 0 - Created: 0 - Modified: 0 - Renamed:
```

only detections that generate an alarm are counted.

IO MONITOR=<Enable | Disable>

Quando il flag è abilitato permette di visualizzare il numero dei file al secondo e al minuto, fornendo informazioni utili per regolare correttamente i valori di soglia nei trigger di allarme e per gestire i comportamenti dei file falsi positivi.

La modalità "IO Monitor" si disattiva automaticamente dopo 1000 rilevamenti, garantendo che non venga utilizzata continuamente ed eccessivamente.

L'utilizzo della modalità "IO Monitor" è prezioso perché consente agli utenti di comprendere meglio le attività del filesystem e di regolare accuratamente i parametri dei trigger di allarme per adattarli alle loro esigenze specifiche di sicurezza.

System Shutdown=<enable|disable>

“System Shutdown” attiva o disattiva la funzione di spegnimento del computer in risposta a un allarme critico. Quando questa funzione è attivata, il sistema si spegnerà automaticamente dopo che AdrenalineRX ha rilevato un'allerta critica, come un tentativo di crittografia di massa da parte di un ransomware.

Il meccanismo di spegnimento automatico è progettato per limitare i danni in caso di attacco ransomware. Quando viene rilevata un'attività sospetta o dannosa che potrebbe compromettere la sicurezza dei dati, l'antiransomware attiva l'allarme critico e, se la funzione di spegnimento automatico è abilitata, il computer si spegne immediatamente per impedire ulteriori danni.

ShutDown e Protezione Reattiva

Questo è un importante strumento di difesa per proteggere i dati sensibili e prevenire la diffusione del ransomware nel sistema, consentendo agli utenti di rispondere prontamente e limitare l'impatto degli attacchi informatici. Tuttavia, è importante utilizzare questa funzione con cautela, poiché lo spegnimento del computer interrompe tutte le attività in corso.

TIPS: *Abilita il flag “System Shutdown” solo quando sei sicuro di aver configurato il file exclude.cfg*

Monitoring Path=<path>

Questo comando specifica il percorso in cui il monitor inizia la scansione in modalità ricorsiva, controllando tutte le sottodirectory all'interno del percorso specificato.

Se il percorso PATH non è definito correttamente AdrenalineRX usa il percorso predefinito è C:\Users\utente\Desktop\

È possibile utilizzare anche lettere di unità come C:, ma questo genera molto rumore. Per ridurre il rumore, è necessario configurare il file exclude.cfg aggiungendo i percorsi rumorosi da escludere dal monitoraggio.

File Limiter=<KiloBytes>

Il campo File Limiter determina la dimensione del primo segmento di dati, o “frame”, che il motore entropico analizza.

Valori di soglia dei campi (*file al secondo e al minuto*):

- Create Ops. /sm = <file per second> <file per minutes>
- Modify Ops. /sm = <file per second> <file per minutes>
- Remove Ops. /sm= <file per second> <file per minutes>
- Rename Ops. /sm= <file per second> <file per minutes>

I campi "Create Ops." consentono di impostare il trigger per gli allarmi di creazione dei file, espressi in secondi/minuto. Quando viene specificato un valore, Adrenaline RX monitora il numero di file creati nel sistema ogni secondo/minuto. Se il numero di file creati supera il valore specificato, viene attivato un allarme.

Esempio: nel pannello di controllo "A::RX" se imposti il campo Create Ops. /seconds = 4 e vengono creati 5 file nel filesystem in un secondo, Adrenaline RX rivaluterà lo score del filtro interno per segnalare un'elevata attività di creazione dei file.

Questo avviso può essere utile per rilevare rapidamente situazioni anomale, come la creazione massiccia di file, che potrebbero essere indicative di un potenziale attacco o di un comportamento sospetto del sistema.

Remove Ops. = <file per second> <file per minute>

I campi impostano il trigger per gli allarmi di rimozione dei file, espressi rispettivamente in secondi e in minuti. Quando viene specificato un valore, Adrenaline RX monitora il numero di file rimossi dal sistema nel periodo di tempo corrispondente. Se il tempo trascorso dalla rimozione di un file supera il valore specificato, viene attivato un allarme.

Tuttavia, è fondamentale valutare attentamente l'utilizzo del comando Remove, quando si configurano i percorsi di monitoraggio, specialmente se si stanno monitorando percorsi del sistema operativo o altre directory ad alto rumore. Ad esempio, se si stanno monitorando i file di sistema del sistema operativo, potrebbero verificarsi frequenti rimozioni di file che non sono necessariamente indicative di un attacco o di un comportamento sospetto. In questi casi, l'attivazione degli allarmi basati sul tempo potrebbe generare falsi positivi e creare confusione.

Pertanto, è consigliabile valutare attentamente la configurazione dei trigger di rimozione dei file, tenendo conto del contesto operativo e delle caratteristiche specifiche del sistema. È possibile ridurre il rischio di falsi positivi regolando i valori dei trigger in base alla frequenza attesa di rimozione dei file nel contesto specifico del monitoraggio. Questo permette di mantenere un equilibrio tra la sensibilità del sistema di allarme e la riduzione dei falsi positivi, garantendo che gli avvisi siano genuini e rilevanti per la sicurezza del sistema.

Per ottimizzare la configurazione dei trigger di rimozione dei file, è consigliabile utilizzare la modalità "IO Monitor" per monitorare attentamente l'attività del sistema. Questo permette di valutare con precisione la frequenza delle rimozioni dei file e di calibrare i trigger nel file config.cfg in modo appropriato.

L'utilizzo della modalità "IO Monitor" consente di adattare i trigger in base al contesto operativo e alle caratteristiche specifiche del sistema, riducendo al minimo il rischio di falsi positivi e garantendo che gli avvisi siano genuini e rilevanti per la sicurezza del sistema.

Max Canary Alarm= <number>

Il campo "Max Canary Alarm" consente di specificare il numero massimo di file Canarino che possono essere erroneamente manipolati dall'utente prima che venga attivato un allarme.

Questa impostazione definisce una soglia di errore per il sistema di allarme rispetto ai file Canarino e conta per tutta la durata della sessione di Adrenaline RX, indipendentemente dai filtri attivi.

Ad esempio, se si imposta "Max Canary Alarm" = 2, significa che devono essere manipolati almeno due file Canarino durante l'intera sessione di utilizzo di Adrenaline RX prima che venga attivato un allarme.

Canary Hide=<enable | disable>

Valore consigliato: disabled

Quando il flag "Canary Hide" è impostato su "enabled" non saranno visibili all'interno di Esplora file (File Explorer) di Windows, a meno che l'utente non abbia attivato l'opzione "Mostra tutti i file nascosti" nel pannello di controllo di MS Windows.

Bottone Edit Canary (canary.cfg) :

Questo file contiene i percorsi e il nome dei file che vengono generati da Adrenaline RX.

Bottone Exclude (Esclude i percorsi dalla scansione):

Una delle funzionalità di Adrenaline RX è la possibilità di escludere determinati percorsi di file dalle scansioni, per evitare falsi positivi o per migliorare le prestazioni durante l'analisi.

Questo è particolarmente utile per percorsi che contengono file di sistema o dati di applicazioni che non richiedono monitoraggio.

TIPS: Abilitando LOG=log1, è possibile monitorare il rumore generato dalle cartelle che non sono state escluse dal monitoraggio. Questo permette di identificare e aggiungere le cartelle rumorose al file exclude.cfg

Schema di Versionamento

Il sistema di versionamento di AdrenalineFX e AdrenalineRx segue uno schema standard composto da quattro numeri:

- Versione principale: Indica una versione significativa del software con importanti modifiche o aggiunte di funzionalità.
- Revisione maggiore: Rappresenta una revisione più piccola rispetto alla versione principale, generalmente caratterizzata da miglioramenti significativi o aggiornamenti importanti.
- Revisione minore: Indica una revisione più piccola rispetto alla revisione maggiore, che include aggiustamenti minori, correzioni di bug o miglioramenti di prestazioni.
- Numero di bug: Rappresenta il numero di bug corretti dalla versione.

Ad esempio, consideriamo la versione "3.5.0100.0":

- "3" è la versione principale.
- "5" è la revisione maggiore.
- "0100" è la revisione minore.
- "0" indica il numero di bug corretti.

Sommario:

Adrenaline CryptoSentinel	4
Introduzione	5
Architettura del Sistema	6
Interfaccia Utente	7
UX-BUFFER:	7
Descrizione dell'Interfaccia Principale.....	8
Bottone Firewall Rules.....	8
Selezione dell'Interfaccia di Rete	10
Opzioni	11
Elenco parametri "UX_BUFFER":.....	11
Elenco parametri "Options":.....	12
Utilizzo per Rilevare esfiltrazioni di dati tramite protocollo di rete.....	13
Interpretazione dei Dati nel Model Viewer e UX-Buffer	15
Pre-Training	16
Utilizzo delle Opzioni di Configurazione	17
Generazione degli eventi in MS Windows.....	19
Gestione del Time-to-Live (TTL) in AdrenalineFX.....	20
Cos'è il Time-to-Live (TTL)?	20
Importanza del TTL in AdrenalineFX	20
Gestione del TTL in AdrenalineFX.....	20
Modelli Dinamici e Variabilità dei Valori (DFP / DPD)	21
Modelli di Riferimento Dinamici	21
Regolazione del "TimeToLive" del Modello	21
Comportamento dei Valori di DFP e DPD	21
Multi-Score Machine Learning.....	22
Metriche Utilizzate	22
DFD	22
DPD	22
Multi-Score Machine Learning.....	22

Consigli per l'Uso	22
Installazione di Sysmon	23
Download e Installazione di Sysmon.....	23
Scarica Sysmon	23
Estrai il Pacchetto	23
Apri il Prompt dei Comandi come Amministratore	23
Installa Sysmon	24
Crea un file dns.xml	24
Modifica il File di Configurazione XML	24
Disinstallare Sysmon	25
Aggiornare Sysmon	25
Installazione dei Driver PCAP per Windows 10	25
Installazione di NPCAP	25
Scarica NPCAP	25
Esegui l'Installer	25
Avvia il file di installazione	25
Installazione di WIN10PCAP	25
Scarica WIN10PCAP	25
Esegui l'Installer	25
Riavvia il Sistema	26
Installare AdrenalineFX CryptoSentinel.....	27
Controllo installazione e verifica	27
Adrenaline RX Engine (Anti-Ransomware).....	29
Introduzione	29
Architettura e Funzionamento di AdrenalineRX.....	29
Entropia del File	29
Byte Magic.....	29
Estensione del File	30
Flusso IO dei File	30
File Canarino	30
Sinergia delle Tecniche di Rilevamento	31
Azioni di Contenimento Estremo	32

Avvio	32
Allarme Sonoro	32
Shut Down Automatico	33
File di Configurazione dei Magic Bytes	33
Installazione	33
File di Configurazione (A::RX)	35
Escludere i percorsi.....	42
Modifica del File exclude.cfg	35
Schema di Versionamento	43