TRUST IN GERMAN SICHERHEIT

G DATA Whitepaper

DeepRay®

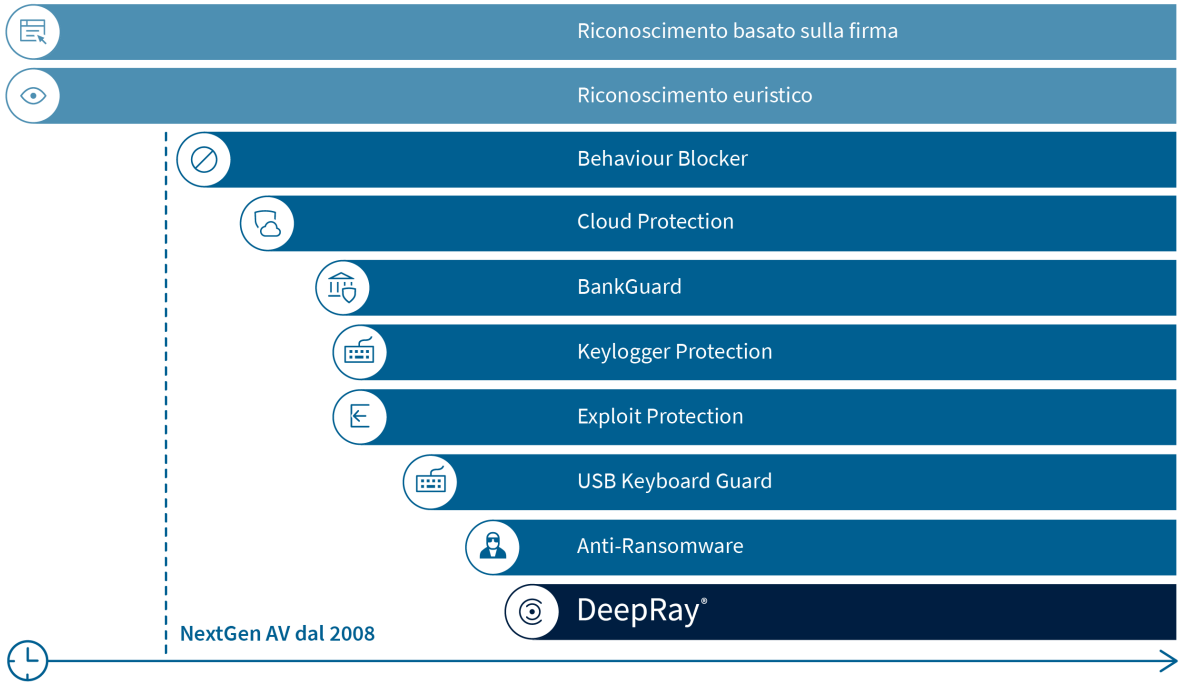
G DATA Software AG

Contents

La IT Security sfrutta l'intelligenza artificiale e il Machine Learning

I cybercriminali e i fornitori di soluzioni di sicurezza informatica si trovano da sempre nella stessa situazione della lepre e della tartaruga della celebre favola. Gli attacchi che utilizzano tattiche note possono essere sventati in maniera più rapida e semplice rispetto a quelli sferrati tramite un nuovo malware. Per questo gli aggressori concepiscono metodi sempre nuovi per superare i baluardi costruiti dalle soluzioni di sicurezza. Gli approcci tradizionali, come le tecnologie di identificazione basate sulla firma, possono soltanto agire in modo reattivo.

Gia dal 2008 la nostra offerta include anche tecnologie next-gen che sono in grado di respingere immediatamente minacce nuove e modificate. DeepRay® protegge gli utenti dalle sofisticate tattiche dei criminali informatici. Le innovazioni tecnologiche che sfruttano intelligenza artificiale, Machine Learning e reti neuronali ci aiutano ad affrontare queste minacce con le giuste armi.



Come viene distribuito il malware agli endpoint?

I criminali che sviluppano malware agiscono su un mercato che si basa su una logica economica tradizionale. Creare malware è molto oneroso e quindi l'investimento deve essere giustificato da un profitto sufficientemente elevato. Per poter realizzare questo utile è necessario che il codice maligno infetti il maggior numero possibile di endpoint. Se però il malware viene identificato, sarà riconosciuto dagli antivirus, non potrà più provocare danni e non sarà più redditizio.

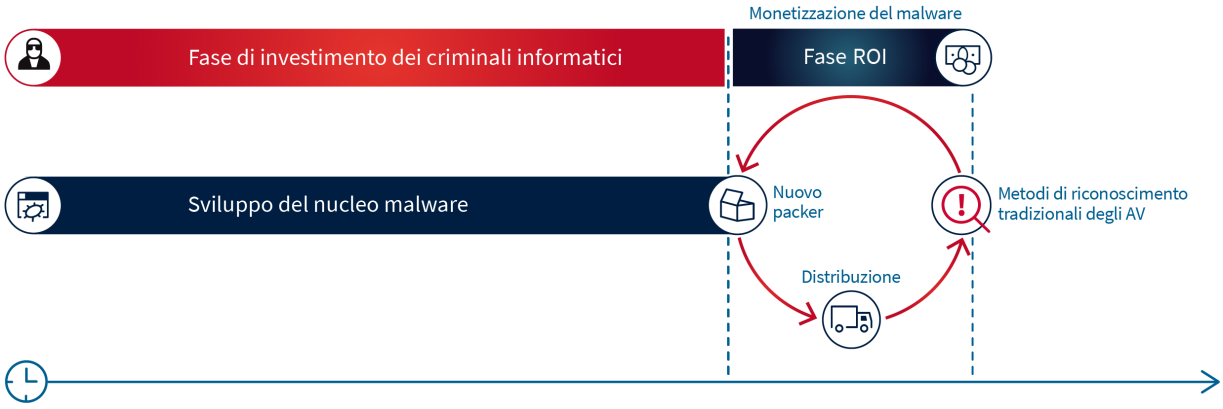
Per non trovarsi nella continua necessità di dover produrre malware, con il dispendio che ne consegue, il codice malevolo viene camuffato. La mimetizzazione è decisamente più semplice (e quindi più economica) e risulta più efficace rispetto alla creazione di nuovo malware. Spesso i programmatori non si occupano da soli né del camuffamento né della distribuzione. Vendono il

malware a numerosi aggressori di tipo diverso che comprimono e distribuiscono i loro nuovi pacchetti agli inconsapevoli utenti attraverso i più svariati canali. Il programmatore può ad esempio ricevere una quota dei riscatto che è stato incassato tramite il ransomware. Questo modello di business, “Ransomware as a service” viene ad esempio messo in pratica dal malware “Grandcrab”, molto diffuso al momento. Sappiamo da specifici forum che il programmatore e i suoi clienti si dividono i proventi dell’estorsione in misura del 60% e 40%.

Il malware usa la tattica della mimetizzazione

Il numero dei packer è già immenso e continua costantemente a crescere. È inoltre possible modificare in maniera rapida e semplice ognuno di loro in modo da ingannare e infine mettere fuori gioco le soluzioni antivirus. In questo caso, gli ostacoli contro cui si scontrano i metodi tradizionali di protezione sono legati a problemi di identificazione.

In alcune circostanze i packer vengono utilizzati in più fasi. Il malware come effettivo nucleo del file eseguibile resta sempre lo stesso. Questo è il modo più proficuo per prolungare la durata di vita del malware e di massimizzare la redditività.

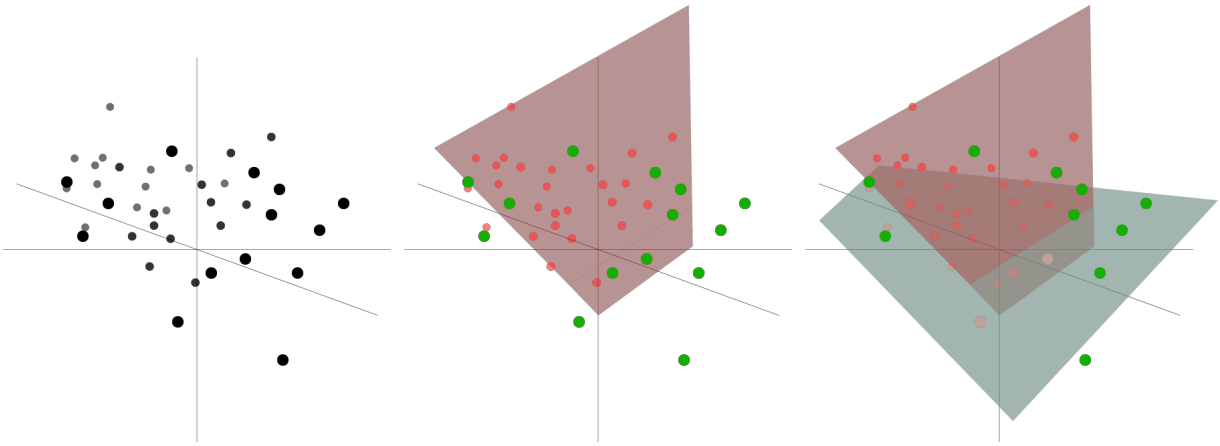


DeepRay® cambia le regole del gioco

Ora con DeepRay® abbiamo sviluppato la tecnologia Machine Learning le cui caratteristiche forniscono a G DATA un vantaggio decisivo rispetto ai concorrenti nella lotta ai criminali informatici. Dopo l’apertura di un malware, che è stato mimetizzato con un packer, il contenuto originale dell’applicazione malevola viene estratto nella memoria. Siccome è impossibile analizzare e valutare in continuazione il contenuto di ogni processo, abbiamo adottato un approccio diverso. La tecnologia che abbiamo sviluppato si avvale dell’apprendimento automatico ed è in grado di capire se un file è stato camuffato oppure no. Quindi il metodo di mimetizzazione utilizzato, cioè il packer, per noi non è più importante e non lo è neppure sapere se il metodo è noto. Gli aggressori dovranno perciò modificare il nucleo del malware con i costi che ne derivano. Una variazione della mimetizzazione sarebbe per loro meno costosa, ma non sufficiente a superare DeepRay®.

Come funziona DeepRay®?

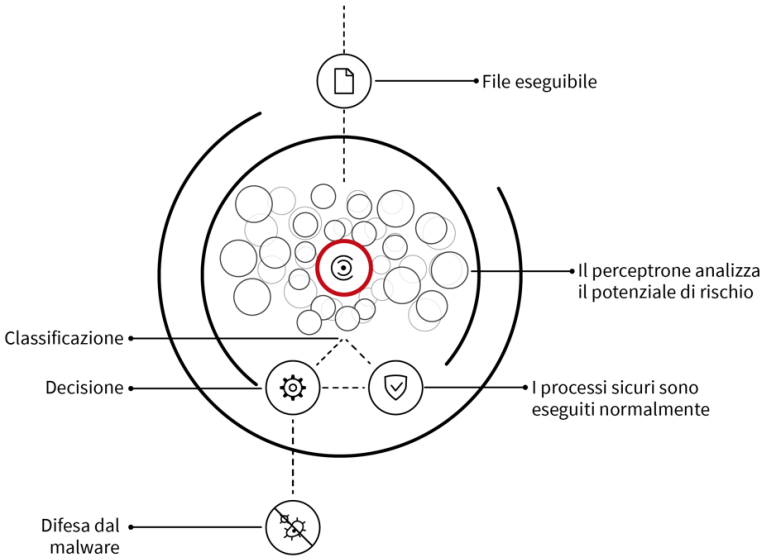
Per la prima fase di identificazione G DATA utilizza una rete neuronale che consta di numerosi perceptroni. In base a molte centinaia di indicatori, questa rete neuronale stabilisce se un file è stato mimetizzato in maniera sospetta prima che il malware venga estratto e riveli il suo nucleo. Esempi di questi indicatori sono le dimensioni dell'intero file e del codice di programmazione contenuto al suo interno, la versione dell'ambiente di programmazione che è stata utilizzata per creare il file oppure il numero delle funzioni di sistema importate.



Come si può vedere dai grafici, i percettroni suddividono le caratteristiche, nel caso di DeepRay® in compresse e non compresse e quindi minacciose o non pericolose. A tale scopo vengono in effetti utilizzati più dei due piani rappresentati in tre dimensioni. Ognuno delle centinaia di criteri corrisponde a un piano e ciò significa che anche la linea divisoria di ogni percettrone attraversa centinaia di piani. Questa grande quantità di piani è anche necessaria per tracciare una linea divisorial affidabile. Il percettrone impara il tracciato ottimale in base a un training set pre classificato. I set vengono continuamente aggiornati per ottenere un risultato di set ideale. Per ottimizzare la precisione del processo in DeepRay®, più percettroni vengono connessi in una rete neuronale.

Difesa rapida contro qualsiasi tipo di minaccia

Se la rete neuronale di DeepRay® stabilisce che un file è sospetto, viene eseguita un'analisi approfondita nella memoria del processo nonché di altri processi probabilmente compromessi. L'identificazione di questi processi è fondamentale, perché il malware spesso tenta di archiviarecomportamenti dannosi in processi di Sistema apparentemente innocui.



Questo metodo di identificazione viene denominato “Taint Tracking”. Per individuare possibili compromissioni vengono monitorate funzioni del sistema che consentono di accedere da un processo all’altro. Se viene registrato un accesso di questo tipo, da quel momento anche il relativo processo viene considerato a rischio (“taint” in inglese significa “macchia”). Questa “macchia” può contaminare a varia profondità altri processi, che saranno anch’essi sottoposti ad analisi. Anche il “fileless malware”, che non viene depositato nel file system, può essere riconosciuto in questo modo.

Nell’ambito dell’analisi profonda vengono identificati modelli che possono essere attribuiti al nucleo di note famiglie di malware o a un comportamento generalmente dannoso.

Un livello di protezione ottimale sin dall’inizio

Per ottenere immediatamente un livello di protezione ideale, abbiamo allenato la rete neuronale con dati di identificazione malware raccolti in oltre 30 anni. Tramite l’analisi di nuove minacce e informazioni provenienti dai SecurityLabs di G DATA, la competenza cresce costantemente e DeepRay® è sempre aggiornato. Inoltre, ogni corretta identificazione dei componenti globali viene utilizzata per il training della rete neuronale. Da ciò risulta un processo di apprendimento adattivo del sistema di IA. I file non pericolosi vengono eseguiti come previsto per consentire all’utente di ottenere le massime prestazioni dal proprio dispositivo. DeepRay® è la più recente tecnologia next-gen delle soluzioni di sicurezza G DATA in grado di riconoscere le minacce in maniera proattiva e prevenire i danni per l’utente.