TRUST IN GERMAN SICHERHEIT

G DATA Whitepaper

DeepRay

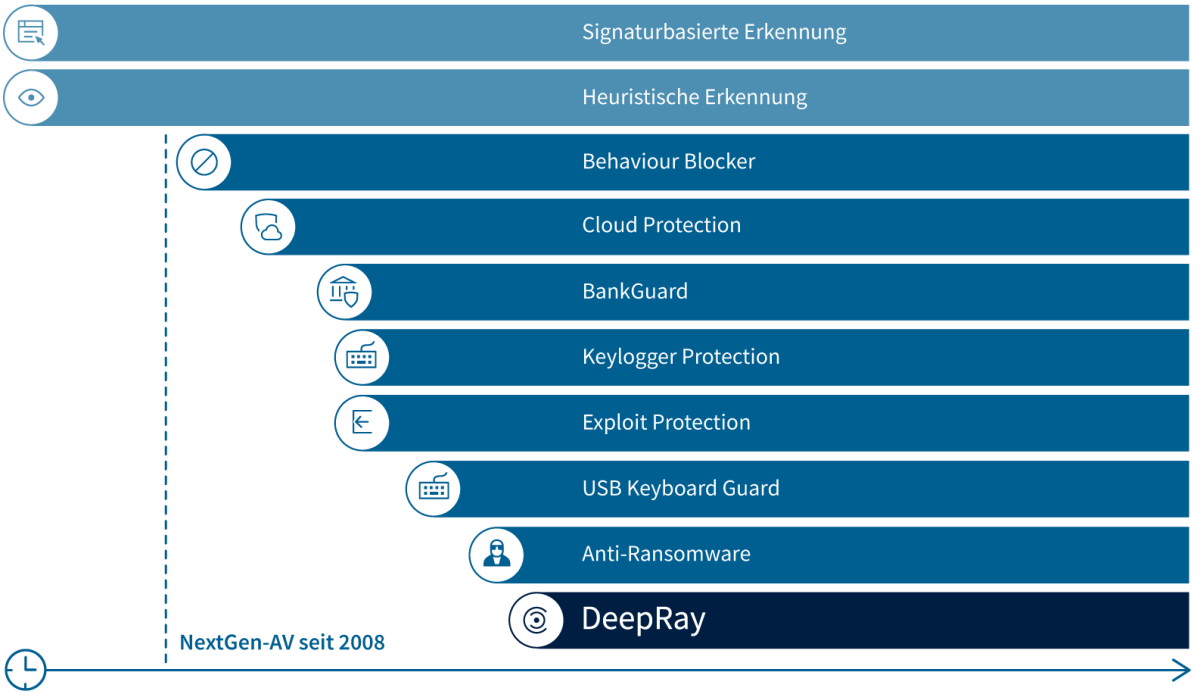
G DATA Software AG | November 2018

Contents

IT-Security nutzt künstliche Intelligenz & Machine Learning

Cyberkriminelle und Anbieter von IT-Sicherheitslösungen stehen sich seit jeher in einer Hase-und-Igel-Situation gegenüber. Angriffe mit bekannten taktischen Methoden können schneller und leichter abgewehrt werden als Angriffe mit neuer Malware. Darum lassen sich die Angreifer immer wieder neue Methoden einfallen, um das Bollwerk, das Sicherheitslösungen aufbauen, zu überwinden. Traditionelle Ansätze wie signaturbasierte Erkennungstechnologien können nur reaktiv agieren.

Bereits seit 2008 beinhaltet unser Angebot auch Next-Gen-Technologien, die veränderte und neue Bedrohungen sofort abwehren können. DeepRay schützt Anwender mit vor den ausgefeilten Taktiken krimineller Hacker. Technologische Innovationen mit künstlicher Intelligenz, Machine Learning und neuronalen Netzen helfen uns, der Bedrohungslage gerecht zu werden.



Wie wird Malware an Endpoints verteilt?

Kriminelle Malware-Entwickler agieren auf einem Markt, der traditioneller Wirtschaftslogik folgt. Malware herzustellen ist sehr aufwendig. Dieser Investition muss ein ausreichend großer Ertrag gegenüberstehen. Um diesen Ertrag zu erzielen, ist es nötig, dass eine Malware möglichst viele Endpoints erfolgreich infiziert. Ist eine Malware aber einmal identifiziert, wird sie von Antivirenlösungen erkannt und kann keinen Schaden mehr anrichten. Die Malware ist nicht mehr profitabel.

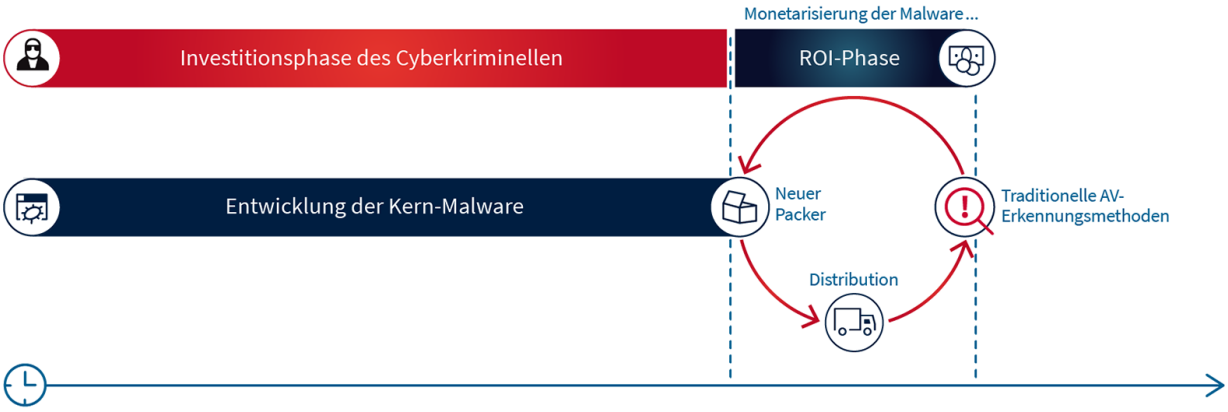
Um nicht immer wieder mit hohem Aufwand neue Malware erstellen zu müssen, wird die Malware stattdessen getarnt. Das Tarnen ist deutlich einfacher – also billiger –, sodass es effizienter ist, als neue Malware zu programmieren. Sowohl für diese Verhüllung als auch für die Verbreitung sorgen die Programmierer der Malware oft gar nicht mehr alleine. Sie verkaufen die Malware an eine

Vielzahl verschiedener Angreifer. Die Angreifer übernehmen das Verpacken und Verbreiten ihrer frisch geschnürten Pakete über verschiedenste Wege an arglose Anwender. Der Programmierer profitiert zum Beispiel über eine Beteiligung am Lösegeld, das mit der Ransomware erpresst wurde. Dieses Geschäftsmodell, „Ransomware as a service“, wird zum Beispiel von der aktuell verbreiteten Schadsoftware „Gandcrab“ praktiziert. Aus einschlägigen Foren ist bekannt, dass der Programmierer und seine Kunden sich den erpressten Erlös 60 zu 40 teilen.

Malware nutzt Tarnung als Taktik

Die Zahl der Packer ist bereits unüberschaubar und wächst weiterhin stetig an. Jeder dieser Packer kann dabei schnell und einfach verändert werden. So sollen Antivirenlösungen getäuscht und letztendlich überwunden werden. Traditionelle Malwareerkennung stößt hier darum auf Hindernisse bei der Erkennung.

Unter Umständen werden Packer auch in mehreren Schichten verwendet. Die Schadsoftware als eigentlicher Kern der ausführbaren Datei bleibt aber immer gleich. Das ist der rentabelste Weg, die Wirkungsdauer von Malware zu verlängern und die Profitabilität zu maximieren.

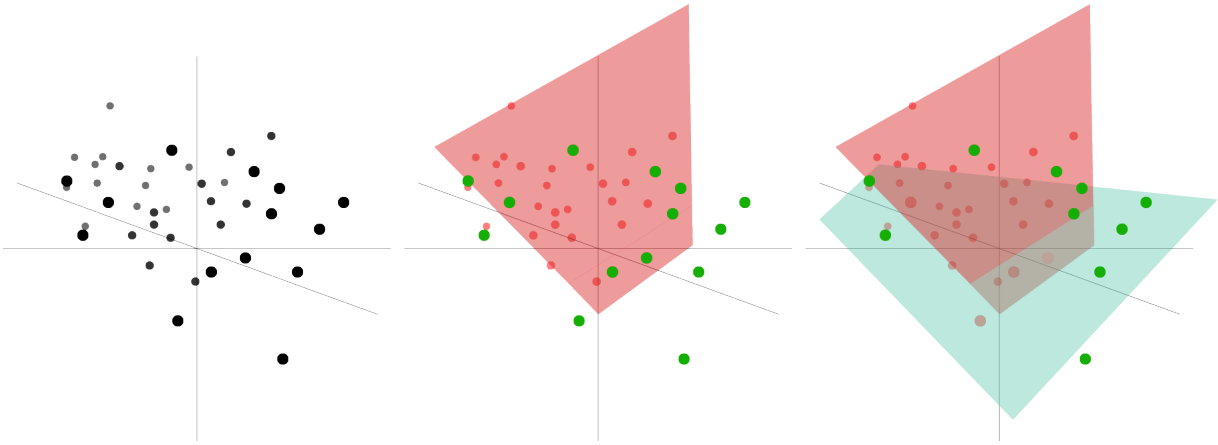


DeepRay ändert die Spielregeln

Mit DeepRay haben wir nun die Machine-Learning-Technologie entwickelt, deren Fähigkeiten G DATA einen entscheidenden Vorteil im Wettbewerb gegenüber Kriminellen verschaffen. Nach dem Start einer Schadsoftware, die mit einem Packer verhüllt wurde, wird der ursprüngliche Inhalt der Malware wieder in den Speicher entpackt. Da der Inhalt jedes Prozesses nicht unentwegt analysiert und bewertet werden kann, haben wir einen anderen Ansatz verfolgt. Die von uns entwickelte selbstlernende Technologie ist in der Lage zu erkennen, ob eine Datei verhüllt wurde oder nicht. Dabei ist es für uns nicht mehr wichtig, welche Verhüllungsmethode, also welcher Packer eingesetzt wird oder ob die Methode bekannt ist. Angreifer müssen daher aufwendig den Kern der Malware überarbeiten. Eine günstige Variation der Tarnung reicht nicht aus, um DeepRay zu überwinden.

Wie funktioniert DeepRay?

Für den ersten Erkennungsschritt nutzt G DATA ein neuronales Netz, das aus mehreren Perzeptren besteht. Anhand von über 150 Kriterien bestimmt dieses Netz, ob eine Datei verdächtig verhüllt wurde, schon bevor sich die Malware entpackt und den Kern offenbart hat. Beispiele für diese Kriterien sind die Größe der Gesamtdatei und des darin enthaltenen Programmcodes, die Version der Programmierumgebung, die verwendet wurde, um die Datei zu erzeugen oder die Anzahl der importierten Systemfunktionen.

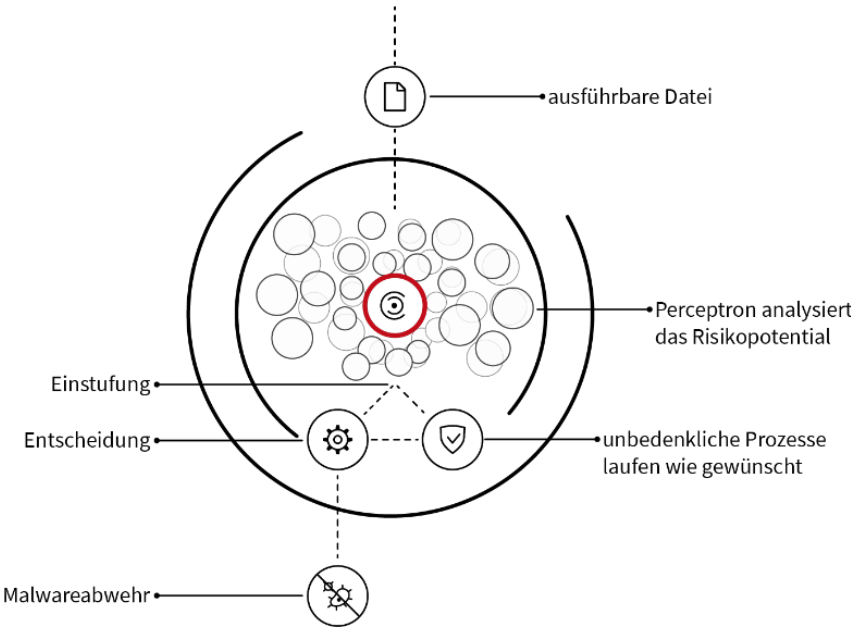


Wie in der Grafik dargestellt, teilen Perzeptren einen Merkmalsraum auf – im Falle von DeepRay in gepackt oder nicht gepackt, und damit bedrohlich oder unbedenklich. Dazu werden tatsächlich deutlich mehr als die dargestellten zwei Ebenen in drei Dimensionen genutzt. Jedes der über 150 Kriterien entspricht einer Ebene, sodass auch die Trennlinie jedes Perzeptrons über 150 Ebenen verläuft. Diese große Anzahl an Ebenen wird auch benötigt, um eine zuverlässige Trennlinie zu ziehen. Der optimale Verlauf wird vom Perzeptron anhand eines vorab klassifizierten Trainingssets gelernt. Die Sets werden für ein ideales Trainingsergebnis kontinuierlich aktualisiert. Um die Genauigkeit des Verfahrens in DeepRay zu optimieren, werden mehrere Perzeptren zu einem neuronalen Netz verknüpft.

Schnelle Abwehr jeder Art von Bedrohung

Entscheidet das neuronale Netz von DeepRay, dass eine Datei verdächtig ist, erfolgt eine Tiefenanalyse. Das geschieht im Speicher des Prozesses sowie möglicherweise kompromittierter anderer Prozesse.

Diese Prozesse zu identifizieren ist wichtig, da Schadsoftware häufig versucht, schädliches Verhalten in



scheinbar harmlose Systemprozesse auszulagern. Die Erkennungsmethode wird als „Taint Tracking“ bezeichnet. Um mögliche Kompromittierungen zu entdecken, werden Systemfunktionen überwacht, die einen Zugriff von einem auf den anderen Prozess ermöglichen. Wird ein solcher Zugriff registriert, gilt fortan auch der betroffene Prozess als gefährdet (Taint – engl. für Makel). Dieser „Taint“ kann in beliebiger Tiefe an andere Prozesse weitervererbt werden. Diese werden dann ebenfalls einer Analyse unterzogen.

Im Rahmen der Tiefenanalyse werden Muster erkannt, die dem Kern bekannter Malwarefamilien oder allgemein schädlichem Verhalten zugeordnet werden können.

Optimales Schutzniveau von Beginn an

Um sofort ein ideales Schutzniveau zu erreichen, wurde das neuronale Netzwerk von uns mit Informationen aus über 30 Jahren Malwareerkennung trainiert. Durch die Analyse neuer Bedrohungen und Informationen aus den G DATA SecurityLabs steigert sich die Leistungsfähigkeit stetig und DeepRay ist immer auf dem aktuellsten Stand.

Darüber hinaus wird jede erfolgreiche Erkennung der Gesamtkomponente verwendet, um das neuronale Netz zu trainieren. So ergibt sich ein adaptiver Lernvorgang des KI-Systems.

Unbedenkliche Dateien werden wie beabsichtigt ausgeführt, sodass Nutzer auf ihrem Endgerät die optimale Leistung abrufen können.

DeepRay ist das neueste Next-Gen-Feature für G DATA Sicherheitslösungen, das Bedrohungen proaktiv erkennt und Schäden für den Nutzer verhindert.