TRUST IN GERMAN SICHERHEIT

G DATA Whitepaper

DeepRay®

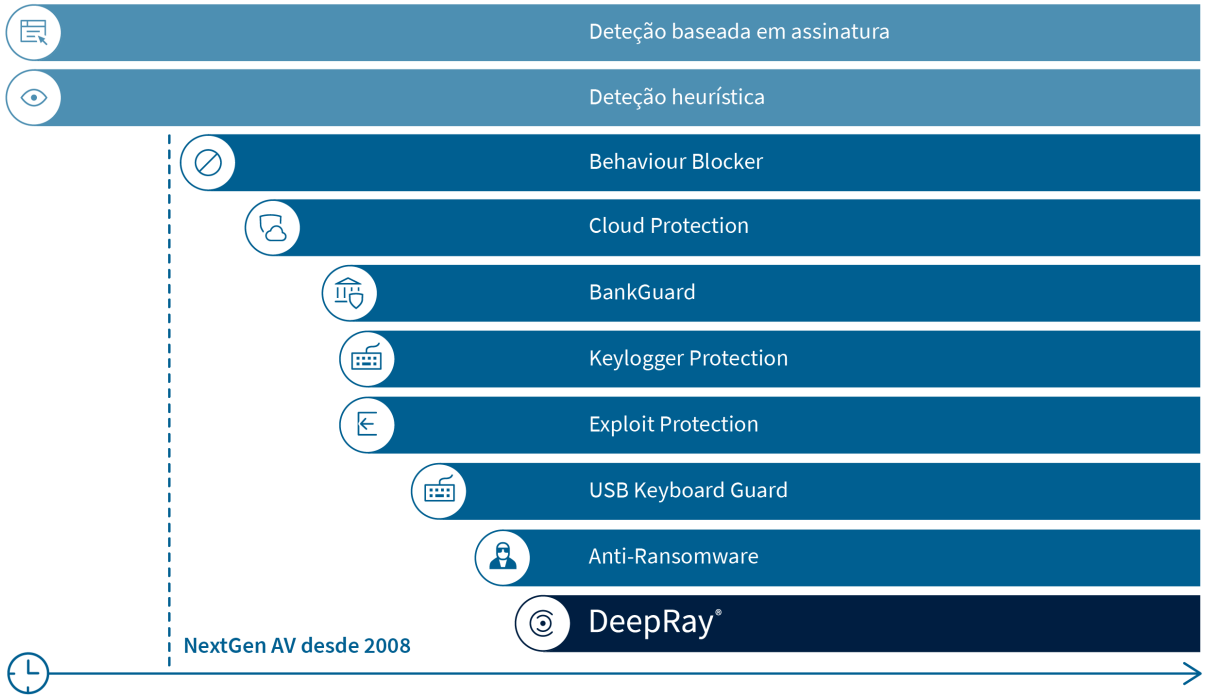
G DATA Software AG

Contents

A segurança de TI aposta em Inteligência Artificial e Machine Learning

Os cibercriminosos e os fornecedores de soluções de segurança de TI sempre se confrontaram com a ideia de que um trabalho bem feito leva tempo e paciência. Os ataques com métodos táticos conhecidos podem ser evitados de uma forma mais rápida e mais fácil, comparativamente a ataques com malware novo. É por isso que os atacantes estão sempre a criar novas maneiras de supercar o baluarte das soluções de segurança. As abordagens tradicionais, como as tecnologias de reconhecimento baseado em assinatura, só podem atuar de forma reativa.

Desde 2008 que a nossa oferta inclui tecnologias de próxima geração que podem neutralizar instantaneamente ameaças novas e modificadas. O DeepRay® protege os utilizadores das sofisticadas táticas de hackers criminosos. Inovações tecnológicas com inteligência artificial, machine learning e redes neurais ajudam-nos a lidar com a situação de ameaça.



Como é distribuído o malware pelos endpoints?

Os programadores criminosos de malware operam num mercado que segue a lógica tradicional de negócios. Desenvolver malware pode ser muito dispendioso. Este investimento deve ser acompanhado por um retorno suficientemente significativo. Para obter esse retorno, é necessário que um malware infete, com êxito, o maior número de endpoints possível. Assim que um malware é identificado, este é reconhecido por soluções antivírus e não pode causar mais danos. O malware deixa de ser rentável.

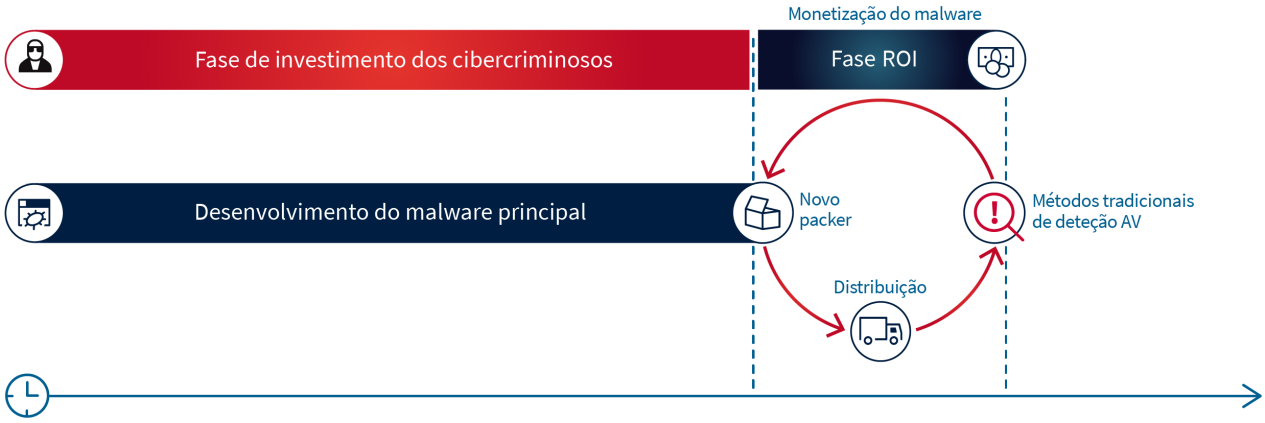
Para evitar criar novos malwares com grande esforço, o malware é camuflado. A camuflagem é muito mais fácil, e como tal, mais barata, acabando por ser mais eficiente do que programar novos malwares. Geralmente, os programadores de malware não lidam sozinhos com esse processo de

camuflagem e distribuição. Estes vendem o malware a diferentes atacantes. Os atacantes tratam da criação de "packages" e da distribuição, por várias vias destes novos pacotes para utilizadores desavisados. Neste caso, o programador recebe uma parte do dinheiro do resgate que foi extorquido com o ransomware. Este modelo de negócio, "Ransomware as a service", é praticado, por exemplo, pelo software malicioso "Gandcrab", o qual é atualmente distribuído e propagado. Sabemos através de fóruns relevantes que o programador e os seus clientes fazem uma divisão de 60/40, respetivamente, dos lucros extorquidos.

O malware utiliza a camuflagem como tática

O número de criadores de "packages" (packers) já é incontrolável e continua a crescer. Cada packer pode ser alterado de forma rápida e fácil. Desta forma, pretende-se que as soluções antivírus sejam enganadas e, por fim, superadas. É aqui que os sistemas de deteção de malware tradicionais encontram obstáculos à deteção.

Em determinadas circunstâncias, os packers também são usados em várias camadas. No entanto, o malware, como núcleo do ficheiro executável, permanece sempre o mesmo. Esta é a forma mais rentável de prolongar o impacto do malware e maximizar a rentabilidade.

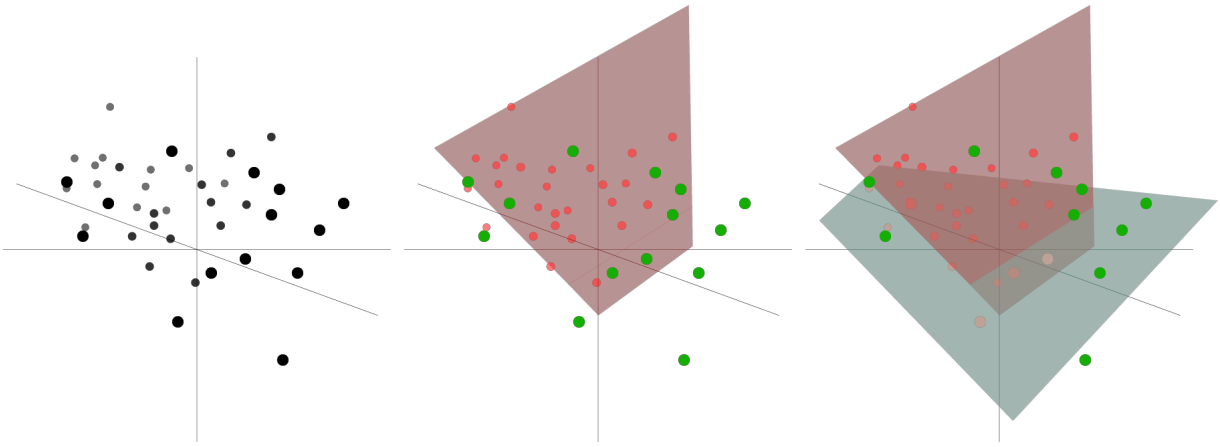


O DeepRay® muda as regras do jogo

Com o DeepRay®, desenvolvemos a tecnologia de machine learning, cujas capacidades fornecem ao G DATA uma vantagem decisiva na luta contra criminosos. Após lançar um software malicioso camuflado por um packer, o conteúdo original do malware é descompactado novamente na memória. Como é impossível analisar e avaliar constantemente o conteúdo de cada processo, adotamos uma abordagem diferente. A tecnologia de self-learning que desenvolvemos é capaz de detetar se um ficheiro foi camuflado ou não. Portanto, deixa de ser importante saber qual o método de camuflagem em causa, ou seja, que packer está a ser utilizado ou se se trata de um método conhecido. Assim sendo, os atacantes têm de reestruturar extensivamente o núcleo do malware. Criar uma mera variante mais barata da camuflagem não é suficiente para superar as defesas do DeepRay®.

Como funciona o DeepRay®?

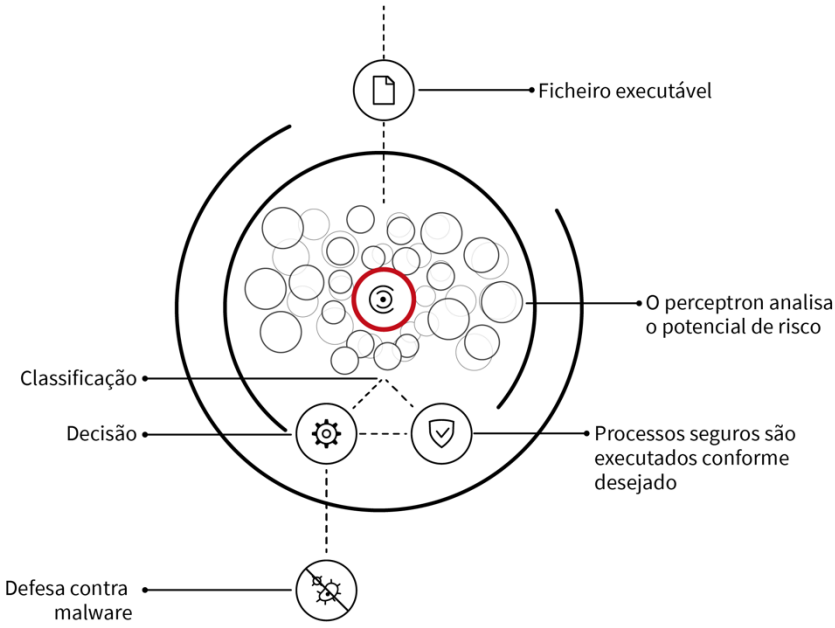
Para a primeira etapa de deteção, o G DATA serve-se de uma rede neural que consiste em vários perceptrons. Com base em várias centenas de critérios, essa rede determina se um ficheiro foi camuflado demaneira suspeita antes mesmo de o malware ser descompactado e revelar o seu núcleo. Estes critérios incluem, por exemplo, o tamanho do ficheiro geral e o código de programação que este contém, a versão do ambiente de programação utilizada para gerar o ficheiro ou a quantidade de funções importadas do sistema.



Tal como indica o gráfico, no caso do DeepRay®, os perceptrons dividem os critérios de aprendizagem automática em compactados ou descompactados e, por conseguinte, em categorias de ameaçador ou inofensivo. Adicionalmente, são utilizados mais do que os dois planos representados em três dimensões. Cada uma das centenas de critérios corresponde a um plano, de modo que a linha divisória de cada perceptron também corre ao longo de centenas de planos. Este grande número de planos também é necessário para criar uma linha divisória fiável. A progressão ideal é aprendida pelo perceptron através de conjuntos de treino pré-classificados. Os conjuntos são continuamente atualizados para assegurar resultados de treino ideais. Para otimizar a precisão do procedimento no DeepRay®, vários perceptrons estão ligados a uma rede neural.

Defesa rápida contra qualquer tipo de ameaça

Se a rede neural do DeepRay® decidir que um ficheiro é suspeito, é realizada uma análise profunda. Tal ocorre na memória do processo e possivelmente noutros processos comprometidos. Identificar estes processos é importante, uma vez que o software malicioso geralmente tenta relocalizar o comportamento prejudicial em processos do Sistema aparentemente inofensivos.



O método de deteção é chamado de "Taint Tracking". A fim de detetar possíveis comprometimentos, são monitorizadas as funções de sistema que permitem o acesso de um processo ao outro. Se tal acesso for registado, o processo afetado será considerado vulnerável (Taint – palavra inglesa para contaminação). Essa "contaminação" pode ser redistribuída para outros processos em qualquer profundidade. Estes são então submetidos, então, a uma análise. Mesmo o "Fileless Malware", que não é armazenado no sistema de ficheiros, pode ser reconhecido desta maneira.

A análise profunda identifica padrões que podem ser atribuídos ao núcleo de famílias de malware conhecidas ou a comportamento geral nocivo.

O melhor nível de proteção desde o início

Para atingir um nível ideal de proteção imediato, desenvolvemos uma rede neural com informações obtidas durante os 30 anos de experiência em deteção de malware. Através da análise de novas ameaças e informações do G DATA SecurityLabs, o desempenho é melhorado constantemente e o DeepRay® está sempre atualizado.

Além disso, qualquer reconhecimento bem-sucedido do componente geral é usado para treinar a rede neuronal. Tal resulta num processo de aprendizagem adaptativo do sistema de IA.

Os ficheiros seguros são executados conforme o esperado, para que os utilizadores possam obter o melhor desempenho do dispositivo.

O DeepRay® é a característica de última geração mais recente das soluções de segurança do G DATA que deteta proativamente ameaças e evita danos ao utilizador.