TRUST IN GERMAN SICHERHEIT

G DATA Whitepaper

DeepRay

G DATA Software AG | November 2018

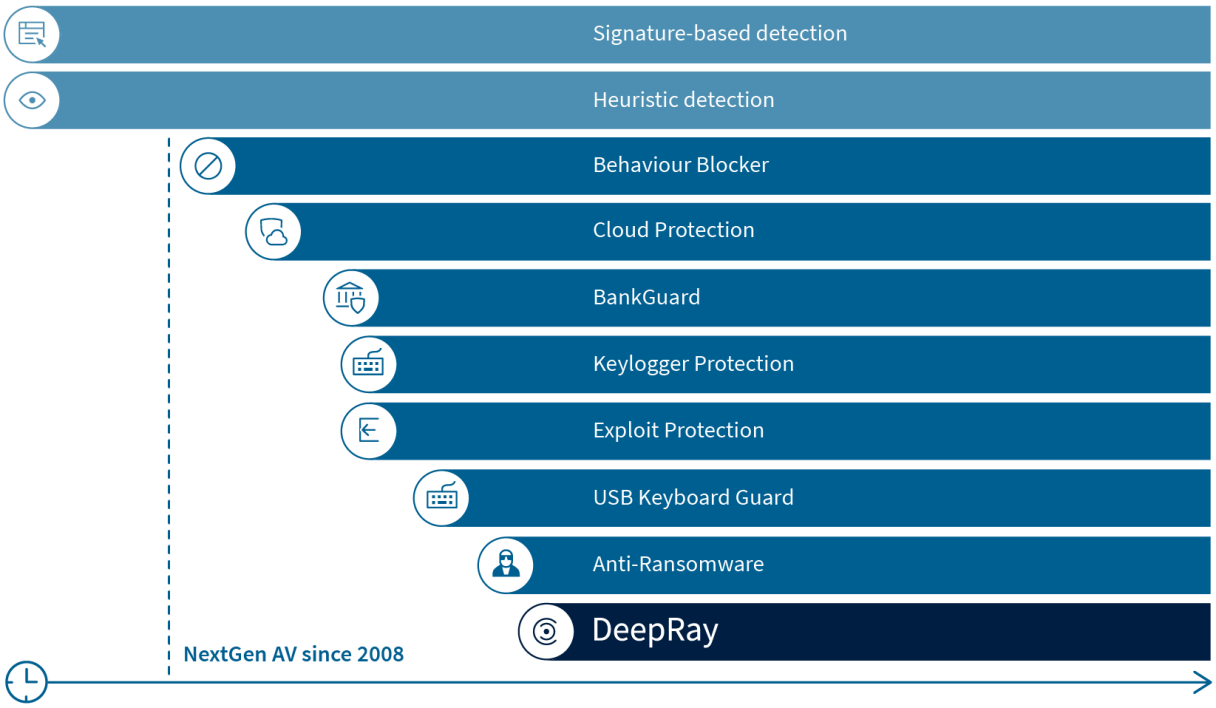
Contents

Copyright © 2018 G DATA Software AG

IT security uses artificial intelligence and machine learning

Cybercriminals and IT security solution providers have always been in a turtle and the hare situation. Attacks with known tactical methods can be foiled faster and more easily than attacks with new malware. Therefore, time and again, attackers come up with new methods to get past the bulwark security solutions build to block them. Traditional approaches such as signature-based recognition technologies can only act reactively.

Ever since 2008, our offer has also contained Next-Gen Technologies, which can immediately fend off both modified and entirely new threats. DeepRay protects users from the sophisticated tactics of criminal hackers. Technological innovations with artificial intelligence and machine learning and neural networks are helping us meet this threat situation head on.



How is malware distributed to endpoints?

Criminal malware developers operate in a market governed by a traditional business logic. Making malware is very expensive, so this investment has to be justified by bringing in a sufficiently great return. In order to achieve this return, the malware needs to successfully infect as many endpoints as possible. But once a malware is identified, antivirus solutions can detect it and it can't do any more damage. The malware is no longer profitable.

To avoid having to create new malware again and again at great expense, the developers simply camouflage the malware instead. Camouflaging is much easier – i.e., cheaper – so it's more efficient than programming new malware. Malware programmers often no longer handle this concealment or the distribution on their own. They sell their malware to a variety of different attackers. The attackers take over the packing and distribution of their shiny new packages to

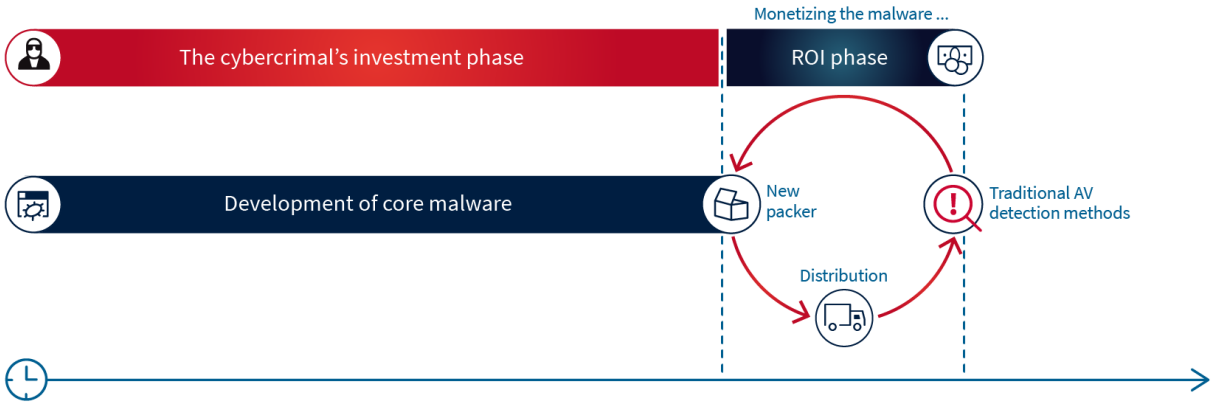
Copyright © 2018 G DATA Software AG

unsuspecting users in various ways. In this case, the programmer gets a share in the ransom money that was blackmailed with Ransomware. This business model, "Ransomware as a service", is used for example by the currently widespread malware "Gandcrab". We know from relevant underground forums that the programmer and his customers get a 60/40 share of the extorted proceeds.

Malware uses camouflage as a tactic

The number of packers is already unmanageable, but it’s steadily continuing to grow. This means that these packers can be changed quickly and easily. So antivirus solutions can be deceived and ultimately overcome. This is where traditional malware runs into obstacles to detection.

In some cases, packers may also be used in multiple shifts. But the malware as the actual core of the executable file always remains the same. This is the most profitable way to extend the active half-life of the malware and maximize profitability.



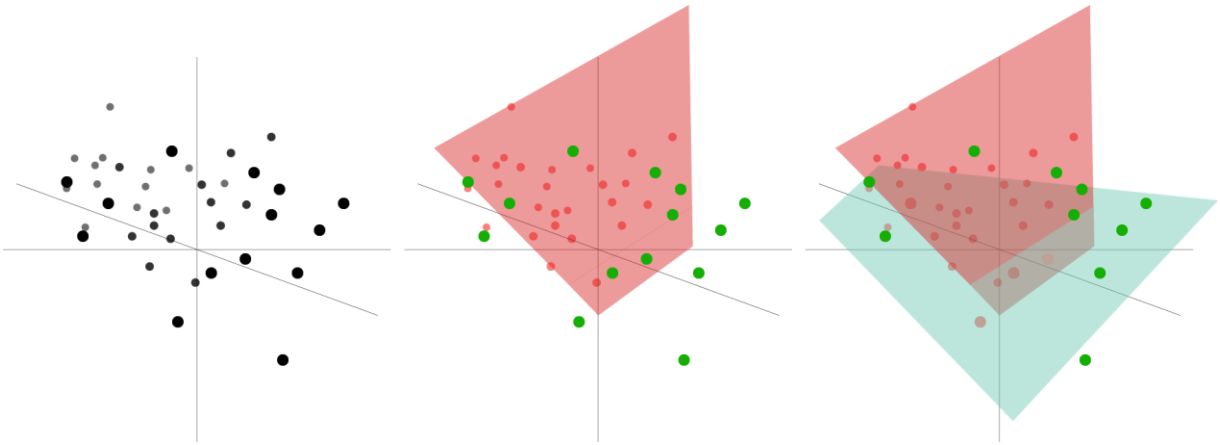
DeepRay is changing the rules of the game

With DeepRay, we have now developed the machine learning technology, whose abilities provide G DATA with a decisive competitive edge against criminals. After a malware has been launched that has been disguised by a packer, the original content of the malware gets unpacked into the RAM again. Since it’s impossible to constantly analyze and evaluate the content of every process, we took a different approach. The self-learning technology we developed is able to detect whether a file has been disguised or not. So it’s no longer important for us to know which disguising method, i.e, which packer is being used, or whether it’s a known method. Attackers therefore have to extensively rework the core of the malware. Simply creating a cheaper variation of the camouflage isn’t enough to get past DeepRay.

Copyright © 2018 G DATA Software AG

How does DeepRay work?

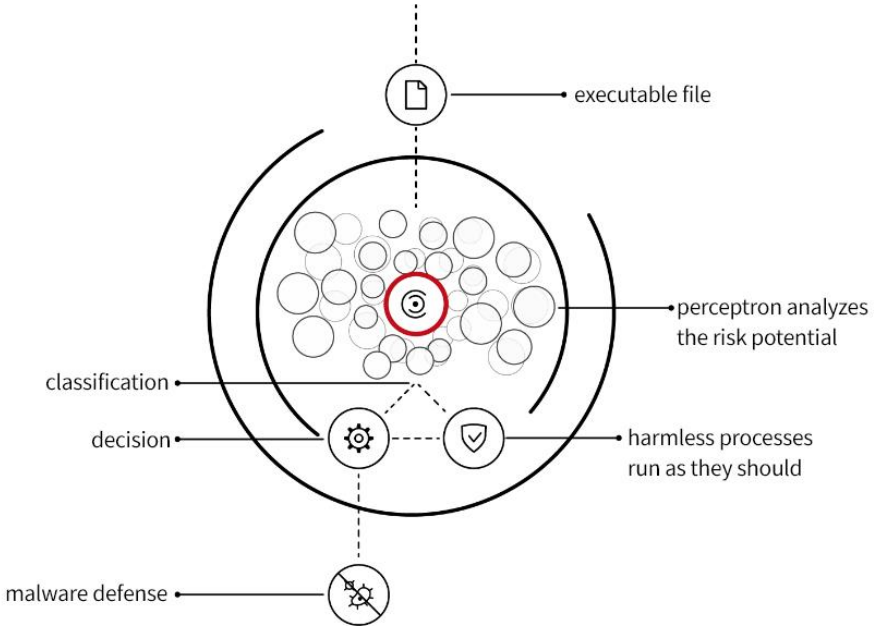
For the first recognition step, G DATA uses a neural network consisting of several perceptrons. Based on several hundred criteria, this network determines whether a file has been suspiciously disguised, even before the malware has unpacked and revealed its core. These criteria can be the size of the overall file and program code it contains, the version of the programming environment used to generate the file or the number of imported system functions.



As shown in the graph, perceptrons divide a feature space – in the case of DeepRay, into packed in packed or unpacked, i.e, into threatening or harmless categories. This actually involved significantly more than the two planes shown in three dimensions. Each of the hundreds of criteria corresponds to one plane, so that the dividing line of each perceptron also runs over hundreds of planes. This large number of planes is also needed to draw a reliable dividing line. The optimal course is learned by the perceptron using a pre-classified training set. The sets are continuously updated for an ideal training result. In order to optimize the accuracy of the procedure in DeepRay, several perceptrons are linked to a neural network.

Fast defense against every type of threat

If the DeepRay neural network decides that a file is suspicious, a depth analysis is performed in the RAM of the process and possibly for other compromised processes. Identifying these processes is important since malware often attempts to relocate malicious behavior into seemingly harmless system processes.



Copyright © 2018 G DATA Software AG

The detection method is called "taint tracking". In order to detect possible compromises, system functions are tracked that allow access from one process to another. If such an access is recorded, the affected process is now also considered to be at risk, or "tainted". This taint can be passed on to other processes at any level. These are then also subjected to an analysis. Even fileless malware that is not stored in the file system can be detected.

This depth analysis involves identifying patterns that can be assigned to the core of known malware families or generally malicious behavior.

Optimal level of protection from the beginning

To achieve an ideal level of protection immediately, we developed a neural network with information gained from over 30 years of malware detection experience. By analyzing new threats and information from the G DATA SecurityLabs, the performance increases constantly and DeepRay is always up to date.

In addition, each successful detection of the total component is used to train the neural network. This results in an adaptive learning process of the AI system.

Harmless files are executed as intended so that users can obtain the optimum performance on their device.

DeepRay is the latest Next-Gen feature for G DATA security solutions that proactively detects threats and prevents harm to the user.

Copyright © 2018 G DATA Software AG