Acronis Leveraging Machine Learning to Secure Data

Introduced in January of 2017, Acronis Active Protection is an advanced technology that uses sophisticated analysis to monitor systems for any ransomware-like behavior and stop it quickly. Even with strong results from independent tests and accolades from the media, Acronis wanted to make the solution more robust. We successfully did so by leveraging machine learning and artificial intelligence technologies.

HOW MACHINE LEARNING HELPS

Machine learning is often a term associated with big data – the analysis of enormous volumes of data to produce actionable results. Since machine learning is based on the amount of data and the algorithms chosen, the larger the data sample, the better the results.

So how does Acronis use this technology? The first step is to conduct a stack trace analysis that reports on program subroutines. This technique is commonly used for certain kinds of debugging, helping software engineers figure out where a problem lies or how various subroutines work together during execution.

Acronis applies this approach to a ransomware attack, using machine learning to detect malicious code injections.

HOW MACHINE LEARNING WORKS

Acronis has analyzed massive volumes of clean data using Windows systems that run scores of legitimate processes. We then obtained millions of legitimate stack traces from these processes and built different models of "good" behavior using decision tree learning. We also collected malicious stack traces from various sources in order to provide counter examples. Based on these millions of learning samples, behavior patterns are identified.

With decision tree learning, we can move from observing an item, to making conclusions about its target value, to creating a model that accurately predicts the value of a new item based on identifiable factors. The models allow Acronis to build-in appropriate responses to target values. Rather than slowing down the client machine by collecting and sending data to be analyzed, the onboard models deliver the same level of protection with greater efficiency.

WHEN IS MACHINE LEARNING ACTIVATED?

As stated above, Acronis Active Protection is based on behavioral heuristics. In version 2.0 we added several new heuristics that look for legitimate processes. If Acronis Active Protection detects strange behavior in a legitimate process, it takes a stack trace and sends it to Acronis' machine learning module. There the behavior is compared with existing models of clean and infected stack traces to determine if it's a threat or not.

If the behavior is determined to be malicious in nature, the user receives an alert suggesting that he block the process.

NEW LEVEL OF ANTI-RANSOMWARE DEFENSE

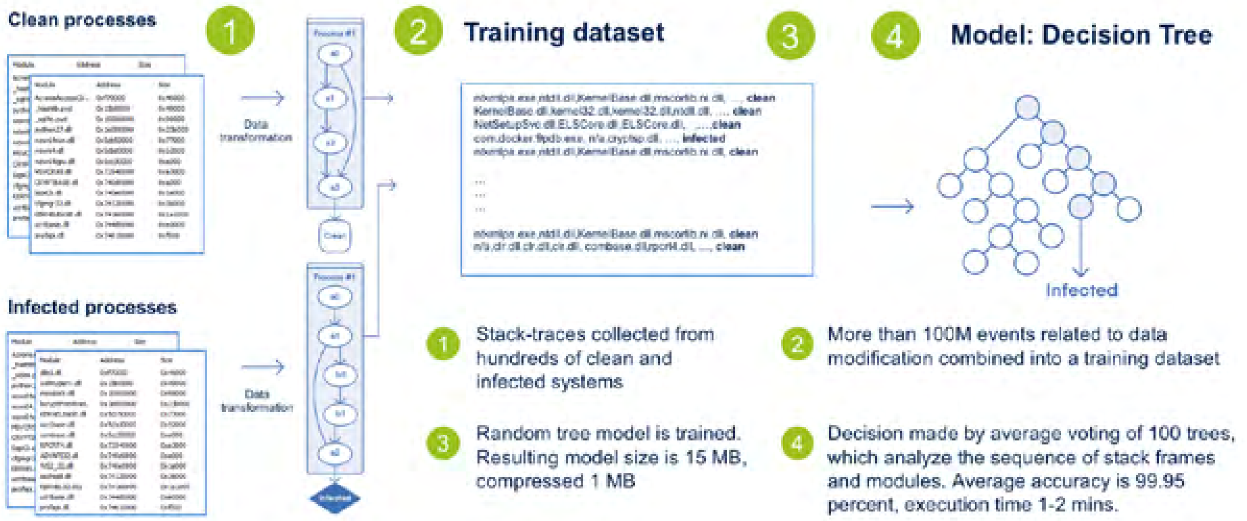
With machine learning leading the way, all of these technologies bring Acronis Active Protection to a whole new level – especially when it comes to combatting zero-day threats. It creates a model for legitimate processes, so even if bad actors find a new vulnerability or way to infiltrate the system, machine learning will detect the ransomware's processes and stop them.

Acronis' machine learning infrastructure is built so that new, anonymized program data is uploaded regularly for analysis. This infrastructure can manage millions of requests simultaneously – and thanks to the constant information flow, new behavior models are ready much faster. Meanwhile, constant updates to product heuristics further boost security. None of this behind-the-scenes, split-second work is noticeable to users – they can simply turn on Acronis Active Protection and forget about it.

WHAT'S NEXT

Acronis continues to expand the use of this technology by utilizing machine learning for static code analysis. This analysis will be done in the pre-execution stage, so when you download a file or copy one to a hard drive, its code will be instantly checked for anomalies. If there is anything suspicious, the process can be blocked before it is launched by a user or an automated script.

Indeed, machine learning models can be used to analyze scripts and Acronis is already working in this direction. In fact, tests by NioGuard Security Lab showed that while most anti-virus solutions are unable to detect a script-based attack, Acronis Active Protection performs well. Despite that success, we will continue making our anti-ransomware technologies even better.



```
mbxmlpa.exe,ntdll.dll,KernelBase.dll,mscorlib.ni.dll, ..., clean
KernelBase.dll,kernel32.dll,kernel32.dll,ntdll.dll, ..., clean
NetSetupSvc.dll,ELSCore.dll,ELSCore.dll, ..., clean
com.docker.9pdb.exe, n/a,cryptsp.dll, ..., infected
mbxmlpa.exe,ntdll.dll,KernelBase.dll,mscorlib.ni.dll, clean

...
...
...

mbxmlpa.exe,ntdll.dll,KernelBase.dll,mscorlib.ni.dll, clean
n/a,clr.dll,clr.dll,clr.dll, combase.dll,rpcrt4.dll, ..., clean
```

1 Stack-traces collected from hundreds of clean and infected systems

2 More than 100M events related to data modification combined into a training dataset

3 Random tree model is trained. Resulting model size is 15 MB, compressed 1 MB

4 Decision made by average voting of 100 trees, which analyze the sequence of stack frames and modules. Average accuracy is 99.95 percent, execution time 1-2 mins.

For additional information, please visit **www.acronis.com**

Acronis