Driving Toward a Better Understanding of Machine Learning

What autonomous cars are teaching us about math-based security strategies

Robert H. Leong
McAfee Labs
The Confusion about Machine Learning

The seismic jolt in the threat landscape caused by the business success of threats like ransomware, combined with the geometric rise of so-called zero-day malware (malware for which no antivirus signature defenses exist), has given rise to an explosion of innovation in the cybersecurity industry. The problem is, a lot of what is being said can be confusing.

One of the most-frequently used phrases in security today is machine learning. You hear it used along with other phrases like analytics and artificial intelligence (AI). These terms are used to describe capabilities, approaches, and strategies, but in reality not many actually understand how analytics (and specifically machine learning) can be strategically applied to the threat landscape.

Put simply, analytics is the scientific process of transforming data into insight for making better decisions. Within the world of cybersecurity, this definition can be expanded to mean the collection and interpretation of security event data from multiple sources, and in different formats for identifying threat characteristics.

Simple explanations of some of the more common terms include:

- **Ransomware**: Malicious software created by a hacker to restrict access to the computer system that it infects and to demand a ransom paid to the creator of the malicious software for the restriction to be removed.

- **Zero-day malware**: A previously unknown computer virus or other malware for which specific antivirus software signatures are not yet available.

- **Machine learning**: The subfield of computer science that gives computers the ability to learn without being explicitly programmed.

- **Artificial Intelligence**: The most complex and intelligent analytical technology, a self-learning system applying complex algorithms that mimic human-brain processes such as anticipation, decision-making, reasoning, and problem solving.

Whether you hear the terms machine learning, analytics, math-based, or AI, they are all a fancy way of saying “statistical comparisons.” We feed the computer a huge collection of data and ask it to do a detailed statistical comparison of features, basically emulating the type of algorithm that we use when deciding what something is.
Driving Toward a Better Understanding of Machine Learning

What Autonomous Cars Can Teach Us

Machine learning works well because malware shares common features, and related clean applications share common features. For an easy analogy, let’s look at autonomous cars. Suppose that they are available and common today and that there is now such a thing as a malicious autonomous car. Such vehicles could be used by terrorists or criminals to do bad things—all sorts of bad things. They could pretend to be taxis and kidnap people. They could drop malicious packages off like bombs (see Figure 1).

Let’s pretend someone could intercept your Uber request, and send a malicious autonomous car to pick you up. You would get in and only realize once you’re in that there is no way to get out of the car.

Robot cars that have been programmed to do bad things
• Suppose that programmable, autonomous cars are common.
• Suppose that they are used by terrorists and criminals to commit terrorism and crimes:
  – Deliver bombs
  – Kidnap people
  – Steal items
• Bad guys “build their own cars” (most of the time).

To relate this back to malware, let’s pretend that the malicious autonomous cars are built in the same factory, just as malware is often built using the same toolkit or family of toolkits. If our usual way of finding a malicious autonomous car involved looking at things like the VIN number and license plate, then a “zero-day” version would alter those numbers so that just looking at it wouldn’t be enough to catch it.

Figure 1. Malicious autonomous cars.

“Catch malicious autonomous cars” = Robot cars that have been programmed to do bad things

<table>
<thead>
<tr>
<th>Type of Features</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Features = “Stuff we can figure out without the car running”</td>
<td>License Plate</td>
</tr>
<tr>
<td></td>
<td>VIN Number</td>
</tr>
<tr>
<td></td>
<td>Year</td>
</tr>
<tr>
<td></td>
<td>Make</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
</tr>
<tr>
<td></td>
<td>Manufacturing Plant</td>
</tr>
<tr>
<td></td>
<td>Component Supplies</td>
</tr>
<tr>
<td></td>
<td>Color</td>
</tr>
<tr>
<td></td>
<td>Date of Manufacture</td>
</tr>
<tr>
<td></td>
<td>GPS Setting</td>
</tr>
</tbody>
</table>

Figure 2. Catching stuff based on static features.

However, you could look at other things that typically go unchanged—like the year, make, and model; when it was made; the weight; and the configuration—to compare it against known malicious vehicles. Basically, static machine learning analysis means we look at things we can figure out without the car running. It’s just parked, and we are looking it over for things that we’ve found in other known malicious autonomous cars. See Figure 2 for examples.

The reason this works is that the bad guys don’t redo the car every time they want to launch another attack, so many of the static characteristics of the car remain the same. You just need to look past the VIN and license plate.
Obviously, you won’t catch all malicious autonomous cars just by looking at the static features. That’s why we can also look at behavioral features, which are things we can figure out when the car is running. What destination did it drive to? Did it drop off any packages? Did it make any calls, and, if so, to whom? Did it pick up packages? Is it using a police scanner or a radar detector to try and evade our detection attempts? See Figure 3 for more examples.

**“Catch malicious autonomous cars” = Robot cars that have been programmed to do bad things**

“Catch malicious autonomous cars” = Robot cars that have been programmed to do bad things

Figure 3. Catching stuff based on behaviors.

The bottom line is this: machine learning is essentially statistical comparison of features. If we have a strategy that accommodates the multiple use cases that attackers are involved with, including changing malware disguises or hiding behind or misusing clean binaries, then we can use machine learning to identify both clean and malicious applications without having a signature.

### Understanding the Issues of “Partial” Machine Learning Approaches

If we go back to the confusion about what machine learning is and why it matters, how and where does machine learning directly impact your environment? Let’s consider malware behaviors that are at the heart of today’s sneakiest attacks. See Table 1.

<table>
<thead>
<tr>
<th>Threat Landscape Problems</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
</tbody>
</table>

Table 1. Market problems.

If we extend our malicious autonomous car analogy, then what would that look like if we mapped the analogy to this list of problems? Well, changing disguises on every PC (or zero-day malware) would be like the bad guys changing the VIN or license plate number. Sandbox-aware would mean that they are using things like radar detectors or police scanners. Piggybacking would be like hiding the malicious car underneath or inside a harmless semi truck. Misuse of clean applications would be similar to reprogramming a known clean car to do something bad.
Driving Toward a Better Understanding of Machine Learning

Table 2. Mapping market problems to the analogy

<table>
<thead>
<tr>
<th>Threat Landscape Problems</th>
<th>Analogy</th>
<th>Strategies Used</th>
<th>Required Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero-day malware is file-based malware that hides using obfuscation (examples: packing, encryption and polymorphism).</td>
<td>Changed VIN or license plate number</td>
<td>Unmask the attack</td>
<td>Look at the stuff that does not change. Look at behavior, and look at the overall feature set.</td>
</tr>
<tr>
<td>Malware is often sandbox-aware (hides from detection by spotting the sandbox and taking evasive actions).</td>
<td>Uses radar detectors, police scanners, checks for presence of &quot;The Matrix&quot;</td>
<td>Unmask the attack</td>
<td>Strip off evasion it while it is still on the computer—force it to reveal itself in a non-sandbox environment.</td>
</tr>
<tr>
<td>Malware evades detection by piggybacking on a known clean application.</td>
<td>Hides the malicious car underneath a harmless semi truck</td>
<td>Unmask the attack</td>
<td>Look at behavior, not appearances.</td>
</tr>
<tr>
<td>Malware evades detection by misusing a legitimate application.</td>
<td>Reprograms a known-clean car to do Something bad</td>
<td>Unmask the attack</td>
<td>Look at behavior, not appearances.</td>
</tr>
</tbody>
</table>

Table 2. Mapping market problems to the analogy

If we then take the market problems and map them against the strategies needed to counter these problems, then you can see the kinds of capabilities that the solution has to have in order to succeed. See Table 2.

To consistently recognize zero-day malware that is sandbox-aware and uses techniques like piggybacking and clean binary misuse, you must employ a speedy machine-learning solution that:

- Unmasks the attack by looking at things that do not change
- Looks at static and dynamic behavioral features
- Strips off the evasion either before or while it is on the PC
- Uses techniques to limit or eliminate damage to the PC (saves patient zero)

Malware Machine Learning Example Design: Real Protect

Real Protect, a McAfee® technology solution, helps enables you to quickly and consistently detect zero-day malware, without antivirus signatures and is based on the machine learning theory we just reviewed.

How exactly does Real Protect do that? It accomplishes this by comparing all features of a file, using both static and behavioral detection methods to quickly and consistently separate what is malware and what is clean. This means:

- **Static analysis detects zero-day malware pre-execution:** Detects obfuscated, polymorphic malware with static attribute analysis comparing to known malware using machine learning.
- **Works in the presence of blocking protection, as well as offline:** Improves detection in conjunction with the use of Dynamic Application Containment or host intrusion prevention, firewalls, or offline.
Driving Toward a Better Understanding of Machine Learning

- **Faster response and a reduced need for human analysis:** Analysis and matching happen very quickly. Because it’s a machine-learning-based system, it is extensible with very few resources.
- **Requires very few resources on the computer:** Both RAM and HDD/SSD requirements are very modest (a few MB).
- **Improves ability to detect malware that can escape static analysis:** Including misuse of legitimate applications, piggybacking on clean applications, and exploitation of vulnerabilities in clean applications.
- **Automated, proactive analysis and classification:** Immediate protection without reactive signatures or human feedback loop.
- **Improves ability to halt suspicious processes “running indefinitely”:** With static-only approaches, a missed detection will result in the suspicious object running.

**Conclusion**

Machine learning is causing both an explosion of innovation in the cybersecurity industry and confusion around best practices. Where it helps most is where we, as humans, struggle to stop enough threats at a fast enough pace with as few resources as possible.

Autonomous cars show us that there is a difference between “things you can figure out when the car isn’t running” and “things you can figure out when the car is running”—and you need both kinds of analysis to catch all threats. Partial machine learning approaches are dangerous and prone to false results.

The best approach is to automatically use static and dynamic detection technologies like Real Protect, which combines multiple sources of security to keep your PC, data, and your identity protected while you are taking full advantage of your digital life.

**Learn More**


About McAfee

McAfee is one of the world’s leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies’ products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.