CYLANCE

EXECUTIVE OVERVIEW

The CISO Series

Transcending Malware: How to Prevent the Initial Attack.

Once cyber attackers gain a foothold in a victim's network they move quickly to entrench themselves in vulnerable systems throughout the network. The cost of remediation once an attack proliferates increases exponentially, and it is compounded by the difficulty of knowing whether the attack actually is contained. Preventing that initial compromise is critical.

Traditional security methods such as signature-based and heuristic anti-virus, and application whitelisting are only minimally effective in defending endpoints against today's increasingly sophisticated targeted and persistent threats.

Machine learning now is being brought to bear on the endpoint security problem. Machine learning offers the promise of more effective endpoint protection and automated mitigation without impacting business processes or user experience.

Unlike the attacks of today, the aim of early malware was simply to cause disruption and invariably prove the point of hackers who had a distaste for the Windows operating system as well as to cause indiscriminate destruction of data.

Malware started its exponential ramp in both quantity and sophistication when attackers discovered how to monetize attacks. Banking Trojans, spam bots, and credential stealing created a growth industry for attackers and defenders alike. It became an arms race.

Cyber criminals would race to develop new malware for newly discovered vulnerabilities. The anti-virus vendors would deploy millions of honeypot accounts, hoping to catch early samples. They also began scanning the web for malware.

As anti-virus solutions were primarily signature-based, cyber criminals developed a number of obfuscation and encryption techniques to change the malware just enough so as not to trigger anti-virus rules.

This arms race passed an inflection point around 2007 when the amount of malicious software outnumbered the total number of good software applications, raising the question of whether it would be better to simply block all executable files except for those known to be good. This approach was termed application whitelisting.

Traditional Defenses Aren't Good Enough

Although a better defense against new malware than traditional anti-virus, whitelisting had its own issues. Enterprises were reluctant to drop one of the primary tools, anti-virus, they had invested significant capital and resources in. What's more, whitelisting applications could put a damper on productivity as workers needed to get legitimate new applications added to the approved list before being able to use them.

Initial deployment of whitelisting solutions was complex and disruptive to the business process and ongoing management of the whitelist was difficult given the advent of Bring Your Own Devices (BYOD) and the increasing complexity of integrated applications. Whitelisting is very broad brushed,

WHY SHOULD CISOS RELY ON MACHINE LEARNING?

- Greater malware detection; upwards of 98% of all data
- Unprecedented and constantly improving accuracy
- Adaptable security to changing attack vectors

often disallowing business critical applications from executing. As well, many whitelisting solutions rely on vendors to maintain their certificates. If a signing certificate was compromised, an attacker could sign malware as trusted and have free reign throughout an enterprise.

Machine learning, based on intelligent and dynamic algorithms, is a new paradigm that shows tremendous promise in rapidly detecting and preventing sophisticated modern attacks. It offers costs savings, resiliency, and future proofing that may well revolutionize endpoint security.

The Power of Machine Learning

"It's not that anti-virus is dead. It's that the paradigm is broken and must be fixed," said IT-Harvest and securitycurrent Executive Editor Analyst Richard Stiennon. "Applying the power of machine learning to the malware problem may be the breakthrough we were looking for to fix this paradigm."

Instead of relying on a long list of malware developed and updated by an anti-virus vendor on a case-by-case basis, machine learning applies advanced algorithms to extremely large data sets from live enterprise environments. On the back end, Cylance is continuously and automatically training its math-based "brain" in a massive data analysis cloud to recognize new abnormalities in code. Even as attackers improve their techniques for hiding malicious code, Cylance is able to pick up on the subtle variations. This develops high fidelity in the malware recognition algorithms, resulting in a low rate of false positives while providing a very high rate of detection. With this approach every endpoint is continuously protected from increasingly sophisticated attacks that are specifically crafted for the target organization.

Cylance Harnesses Machine Learning

Cylance has transcended the old model of determining signatures of good and bad software through a combination of manual and automated analysis. Cylance has turned to the power of machine learning to secure endpoints and prevent the initial attack.

Cylance brings intelligent predictive analysis to bear on today's most difficult security challenges using cutting edge machine learning techniques. By examining thousands of variables in hundreds of millions of samples, they have literally taught a gargantuan machine the difference between good and bad. Simple criteria are applied to all the elements of an executable to determine which might indicate the existence of a piece of malware. Because all malware, even those that attack a previously unknown vulnerability, have similar traits it also is possible to catch zero-day malware with machine learning.

The time is right for this approach according to securitycurrent Principal Analyst, Steve Hunt.

"Making long lists of good and bad sites, good and bad code, always seemed like a losing battle. Malware has shown itself to be tremendously adaptable, morphing into a new variant as soon as our lists tag it as malicious. Machine learning is closer to how we all make decisions, on the fly, from the gut," Hunt said.

While the machine learning process is extraordinarily computationally intensive, the actual detection and prevention on the endpoint through the use of mathematical algorithms consumes far less time and resources than traditional signatures. Cylance does the calculations on the host, in real-time to determine what is safe and what is a threat with the option to block the threat before it can execute. Its future proof, not by looking at a bunch of endpoints for what's bad after the attack. That's the old AV model. Rather, Cylance approach is to have continuous collection of threat and good data analyzed in its math 'brain' in the cloud. Then the machine learning performs ongoing analysis to identify any net new abnormalities and changes in threat behavior. Only then does it modify the algorithms to ensure high fidelity of accuracy.

This Executive Overview is sponsored by Cylance. For more information on Cylance visit www.cylance.com

CYLANCE'S APPROACH PROVIDES:

- Prevention of malware execution
- Low end-user impact
- Centralized management of corporate and personal devices

securitycurrent.com

securitycurrent