BROADCOM

Knowledge is power in the fight against cyberthreats

Attackers are constantly changing their tactics, but expert insight into their game plans can give defenders the advantage

Dick O'Brien
Broadcom

"THE OLD-FASHIONED WAY OF BLOCKING ATTACKERS ISN'T AS EFFECTIVE AS IT USED TO BE. DEFENDERS HAVE TO IDENTIFY MALICIOUS BEHAVIORS RATHER THAN MALICIOUS FILES."

A decade or so ago, keeping the bad guys out was just a matter of blocking malware, viruses and Trojans, but attacks have evolved significantly. Now government agencies and other organizations are facing sophisticated nation-state attacks and high-level cyber crime.

Although attackers have different motives, they have to go through certain steps to achieve their objectives. They will seek to gain access to the targeted network, pursue privilege escalation to acquire administrative credentials, move laterally from one computer to another on the network, and exfiltrate data.

Over time, attackers have reduced the amount of malware they use because they can now rely on legitimate software to achieve their goals. Sometimes they install that software themselves, and sometimes they use software that's already on their target's network, a tactic known as living off the land. As a result, the old-fashioned way of blocking attackers isn't as effective as it used to be. Defenders have to identify malicious behaviors rather than malicious files.

Understanding the impact of AI

As artificial intelligence becomes widespread, we're seeing evidence that some attackers are using AI to write malicious code, but AI is having a bigger impact on the creation of phishing materials because of its ability to churn out convincing content.

Nevertheless, the real game changer is the advent of AI agents. Within weeks of OpenAI releasing its Operator tool, Symantec's Threat Hunter Team did an experiment. We gave Operator my job title and told it to identify the person who performed that role, find my email address, create a malicious PowerShell script designed to gather systems information, and email it to me with a convincing lure.

Operator followed those instructions with little effort on our part. This experiment showed that AI agents are lowering the barrier to entry for attackers, and those agents will only become more powerful.

Sharing threat intelligence as widely as possible

On the defense side, Broadcom has been using AI for over a decade. We started by creating an analytical tool that was trained on all the threat investigations we did over the course of five or six years. That tool is capable of identifying patterns of malicious activity. We use it ourselves and have also baked it into our products so customers can see the alerts and act on them.

Most recently, we have taken inspiration from how generative AI

works and developed a tool called Incident Prediction. When a breach is discovered on a network, Incident Prediction can identify the next steps that attackers will take, allowing responders to identify the areas of concern and close them off. They can take targeted action without being overly disruptive.

In addition, Broadcom shares a variety of threat intelligence with our customers so they can hunt through their networks for indicators of compromise and act on them. Even when customers rely on other vendors for some of their security tools, they can use our threat information across solutions.

We also produce threat alerts that share key indicators of compromise from recent attacks and offer a threat intelligence API that users can query for information about a specific file or network address, for example, to see how prevalent it is and whether we consider it malicious or benign.

All those offerings demonstrate our commitment to share threat intelligence as widely as possible so the cyber defenders can outsmart the attackers. ■

Dick O'Brien *is principal intelligence analyst for the Threat Hunter Team; a group of security experts within Broadcom whose mission is to investigate targeted attacks, drive enhanced protection in Symantec and Carbon Black products, and offer analysis that help customers respond to attacks.*