https://www.darkreading.com/threat-intelligence/deception-a-convincing-new-approach-to-cyber-defense/a/d-id/1329839?

9/12/2017
10:30 AM

Ofer Israeli

Deception: A Convincing New Approach to Cyber Defense

How defenders in a US national security agency capture-the-flag exercise used an endless stream of false data across the network to thwart attackers and contain damage.

We live in a reality of continually multiplying attack vectors. Hackers are using increasingly brazen methods to break past perimeter defenses, using stolen credentials and backdoors, phishing, spyware and malware, brute force, and more. Once attackers have successfully breached a network, they typically have plenty of time to do significant damage. According to the Verizon 2016 Breach Investigations Report, only about 25% of compromises were discovered in "days or less," and the 2017 FireEye M-Trends report indicates that despite continuing improvement, the median number of days attackers dwell in victim networks before discovery is still 99 days — over 3 months — with 47% of breach notifications coming from external sources (such as when the FBI comes knocking).

No single solution can possibly prevent all forms of attack while also limiting the damage of a successful attack. Like a military composed of an army, navy, and air force, each with multiple types of weapons and personnel, a cybersecurity defense system must anticipate all possible threat vectors and develop specific and often multiple mechanisms for combating each.

Awareness of deception, one of the latest cyber innovations, is increasing. Gartner calls it "threat deception" and predicts 10% of enterprises will employ some form of cyber deception by 2018. [Editor's note: The author is the CEO of one of a number of vendors that are actively marketing threat detection products.] Deceptions rely on one of the few vulnerabilities attackers have: They believe that what they encounter on the network is real and that the data they collect is reliable. The deceptions strategy leverages this and layers enterprise endpoints, networks, data, and applications with false information that looks real to attackers. When perimeter defenses fail — and they will — attackers can't differentiate between the real data and the deceptions.

Consider how most sophisticated attackers approach a network. First, unlike movie portrayals, these hackers are slow and methodical, using various tools and techniques to collect data, analyze it, and move laterally throughout a network. Initially, when accessing a network, they are at a bit of a loss. They don't know where they have landed or where the target is. Through trial and error, they build a map of the environment — both the network itself and how it is used. For example, from one employee's PC, they may hit a SharePoint server, where they find documents and names of interest, which helps them determine where they should move next. The more sophisticated the attackers, the more tricks they have to move laterally, and the more they move around, the more detailed the map. This iterative process eventually enables them to find and breach their target.

One common strategy used today to catch attackers as they move around the network is honeypots. Honeypots look like PCs or servers, and the idea is that when attackers access a honeypot, an alarm is set off, alerting IT to the attack. The problem with honeypots is that they are time-consuming to deploy and manage, so relatively few are used, which means significant compromise already may have occurred by the time one is accessed. Even worse, they are actually easy for experienced hackers to identify.

Deception & Capture-the-Flag

Threat deception takes a different approach. Describing the progression of a red-team exercise demonstrates it best, and also shows the effectiveness of deception as a technique. A US national defense agency set up a capture-the-flag exercise to test the effectiveness of a deception strategy. One team took an offensive role, trying multiple attacks to capture and retrieve a target being protected by the defensive team. The offensive team did not know that a deception strategy was being deployed. The defensive team then introduced an endless stream of different sets of false data across the network — on endpoints, servers, and attack surfaces. The types of deceptions included "share deceptions" that dupe attackers to access fake shared folders and files, "Windows credentials deceptions" that ensnare attackers with non-existent user credentials, and "file deceptions" that induce attackers to access and use credentials stored in fake files. The deceptions were carefully crafted for the agency to ensure they would seem real to the attackers.

To deploy the deceptions, the defensive team used two components, a server to distribute the deceptions, and a trap server. As a low-footprint, agentless solution, the deception strategy had almost no impact on network services and performance and was potentially highly scalable. The deceptions were deployed on existing workstations, laptops, and servers throughout the enterprise, requiring no special hardware. Further, legitimate users of the network never accessed the false information, so they were able to continue working unaware and uninterrupted. This also dramatically reduced the number of false positives for the defensive team.

When the offensive team launched its attack, it immediately and unknowingly encountered the deceptions, which appeared identical to what the team needed for moving laterally across the network. Accessing the deceptions triggered the trap server, which alerted the defensive team to the attack. The trap server acts like a real server; when encountering it, the attacker sifted through the information it contained, as an attacker normally would do, but of course in this case the data was false. The trap server also ran real-time forensics on the source of the attack, helping the defensive team to determine the attacker's goals and deliver actionable evidence and artifacts to help them contain the incident. In a real attack, the forensic analysis might also have been very valuable to law enforcement.

Similarly, a large international bank, concerned about the rising number of advanced persistent threats targeting financial services institutions, also deployed a deceptions strategy to complement its other existing cybersecurity tools and to add a new, more immediate threat detection capability. The bank used a similar approach to the US national defense agency, deploying a range of deceptions for shared folders, servers, Windows credentials, SWIFT, and other network systems. With the deception solution in place, the bank achieved its goal of nearly instant detection with a very low rate of false positives. When an alert was triggered, the security team was able to watch the attacker's attempts to move laterally through the network, gather forensic data, and monitor the attack in motion. This enabled the team to be more strategic and stop the attack before it caused damage.

Cybercriminals will continue to get smarter and bolder. To protect your network, you must continue to strengthen your defenses. Deceptions add a powerful, preemptive, complementary defensive solution against advanced attacks. If it's your job to ensure the security of your network and data assets, you should give deceptions a look.

https://www.darkreading.com/author-bio.asp?author_id=2528

Profile of Ofer Israeli

CEO & Founder, illusive networksNews & Commentary Posts: 2

Having pioneered deception-based cybersecurity, founder and CEO of illusive networks Ofer Israeli leads the company at the forefront of the next evolution of cyber defense. Prior to establishing illusive networks, Ofer managed development teams based around the globe at Israel's seminal cybersecurity company Check Point Software Technologies, and was a research assistant in the Atom Chip Lab focusing on theoretical Quantum Mechanics. Ofer holds B.Sc. degrees in computer science and physics from Ben-Gurion University of the Negev.