lifehacker IT PRO | Australia

http://www.lifehacker.com.au/2016/09/security-by-deception-a-different-approach-to-instruction-detection/

Security By Deception: A Different Approach To Instruction Detection

26/09/16

ANTHONY CARUANA *TODAY 3:30 PM*

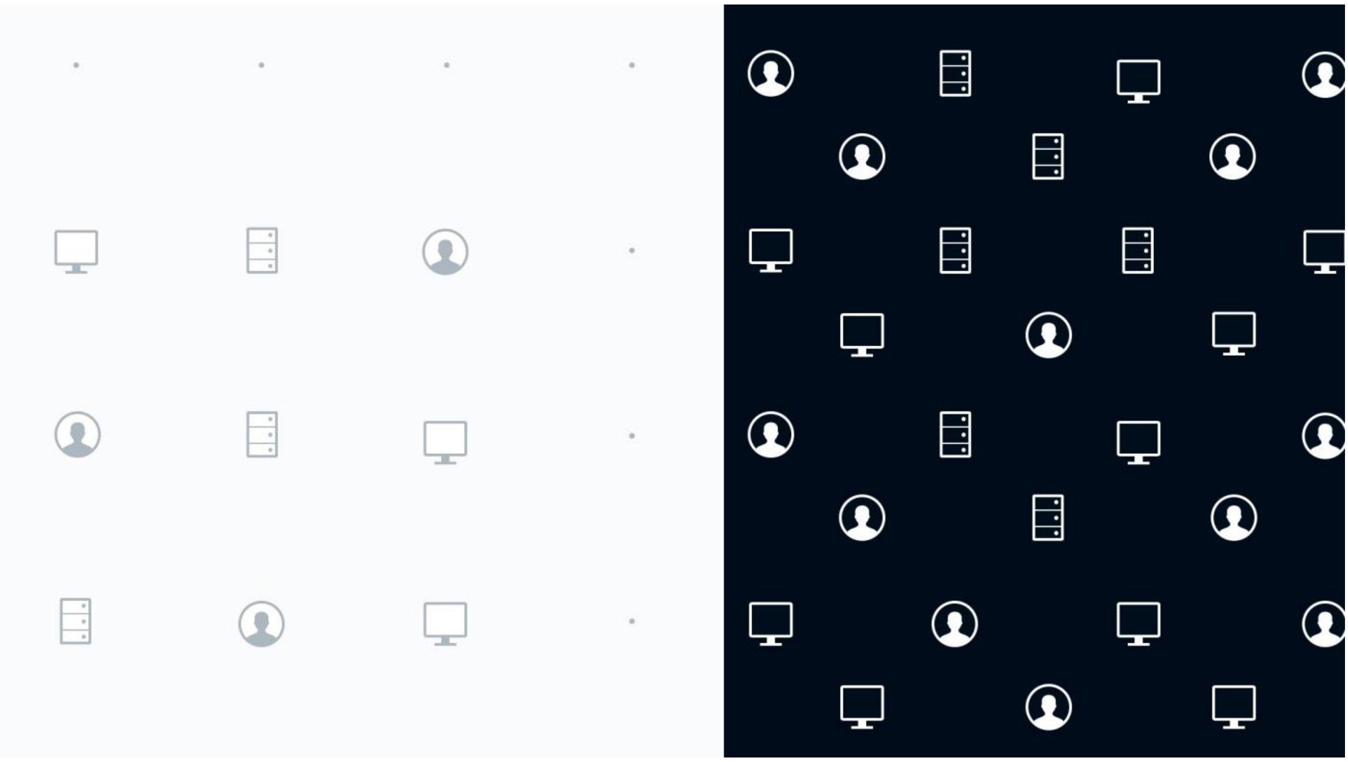

Image: Javelin Systems

Traditional instruction detection systems rely on systems that collect data when actual devices or applications are infiltrated. Some security experts advocate the use of honeypots, to lure bad guys into systems that look valuable but are simply decoys. But a new start up is taking a different approach.

Javelin focuses their efforts on the "detect" part of the Protect-Detect-Respond cyber threat chain. I spoke with Javelin's COO Greg Fitzgerald at the NetEvents Global Press and Analyst Summit.

When attackers breach an end point, their first move is to quietly move around the network, looking for another vulnerable machine or service. If you're on a network with a hundred machines, the attacker will probe those machines until they find a hole and keep going until they hit your crown jewels.

Javelin's way of thwarting the bad guys is to mask the entire network topology using a technology they call "ZeroMove".

ZeroMove creates thousands of virtual honeypots on your network. So, when the attacker is in your network and starts moving laterally, all they hit are fake machines that only exist in memory – they don't use any physical or virtual systems like conventional honeypots. When the bad guy hits one of the fake targets – Javelin's play here is based on the very strong probability that the attacker will hit one of the many fake machines rather than a real target – an alert is sent so your security responses guys can react.

The benefit here is the bad guys aren't actually dropped from your network. Rather, they think they have hit a good target and remain active allowing security teams to carry out forensics so they can track the threat actors and block future attacks.

Whether Javelin's method works in the long-term is still a question I have. Many security teams were fans of security tools that spun up virtual machines in order to explode potentially dangerous payloads. But the bad guys struck back with malware that was able to detect if it was being executed in a VM. Whether the same fate awaits Javelin is something I'd watch out for.

Anthony Caruana attended the NetEvents Global Press Press and Analyst Summit in Silicon Valley as a guest of NetEvents