CounterTack®

Security Brief

Security Challenges in the New Threat Landscape

New and unknown threats are becoming more complex and are increasing the workload for security professionals. Security teams are faced with a continuous stream of new malware, ransomware and fileless attacks that put their organization's sensitive data and business operations at risk. To combat these threats security teams need to look to new technologies and procedures to strengthen their security profiles and protect their assets.

Over 357,000,000 new malware variants.

49% of all cyberattacks are now fileless

In 82% of security incidents the initial compromise only took minutes

Average time between initial compromise and breach fixed is 229 days

New Malware is Running Rampant

According to AV-Test, an independent research organization, a new malware specimen emerges every 4.2 seconds. The April 2017 Symantec Internet Security Threat Report found similar results. Their research estimates there were over 357 million new malware variants introduced last year. Symantec also identified ransomware as the fastest growing malware with 101 new families and 241,000 new variants. The WannaCry, NotPetya and Bad Rabbit attacks demonstrate that businesses are now a prime target. These new threats can cost millions in fines, legal fees and settlements, as well as lost revenues from damage to brand and reputation.

Cybercriminals are also turning to fileless attacks. By injecting malware direct into memory or utilizing "living-off-the-land" techniques, they are able to evade detection from legacy endpoint security solutions. The Verizon 2017 Data Breach Investigation Report determined that 49% of all cyberattacks are now fileless. The success of these techniques means that unknown attacks now pose the biggest security risk. According to Verizon, over 90% of the security breaches they investigated where not previously seen by security teams.

Legacy endpoint solutions like Antivirus, Next Gen Antivirus and event-based Endpoint Detection and Response solutions are effective at catching known threats. They are not effective at catching unknown threats and fileless attacks.

Security Teams Are in a Race Against Time

Any latency in detection and response time increases the exposure of sensitive data and business operations. The problems is today's attacks are fast moving and rerapid detection, analysis and response. According to Verizon, in almost 82% of security incidents the initial compromise only took minutes. When events happen that quickly, security teams struggle to keep up. Ponemon estimates the time between an initial compromise, the lateral movement of an attack through the network and when the breach is fixed averages 229 days. In order to limit the damage, security teams need to implement strategies that reduce response times down to minutes.

Unfortunately, by the time vendors identify and update signatures and IoCs (Incidents of Compromise), new and unknown attacks could be well underway, causing severe damage. In addition, forensic investigation into unknown and fileless attacks are time consuming. The cycle times associated with running forensic tools, quarantining endpoints and analyzing log files delay timely response.

Forward-thinking Security Teams Look to New Solutions

Security teams recognize the need for new technologies and procedures to strengthen their security posture and survive in the new threat landscape. They are turning to a new class of endpoint security solutions: Behavioral Endpoint Detection and Response (EDR). CounterTack's Endpoint Threat Platform is the only true Behavioral EDR solution available today. It does not rely on signatures or IoCs and therefore is the most reliable solution for detecting and responding to unknown threats and fileless attacks.

The bottom line: CounterTack's Endpoint Threat Platform detects the most threats, with the fewest false positives, for the fastest response. It empowers security teams with the intelligence needed to prioritize threats and to adopt more agile and proactive threat management strategies required to protect sensitive data and ensure uninterrupted business operations.

What You Need At a Glance:

CounterTack Endpoint Threat Platform

- The only true behavioral EDR solution.
- The most reliable solution for detecting and responding to unknown threats and fileless attacks
- Delivers the intelligence needed to prioritize and respond to threats faster and more accurately
- Enables adoption of agile and proactive threat management strategies
- Protects sensitive data and ensures uninterrupted business operations