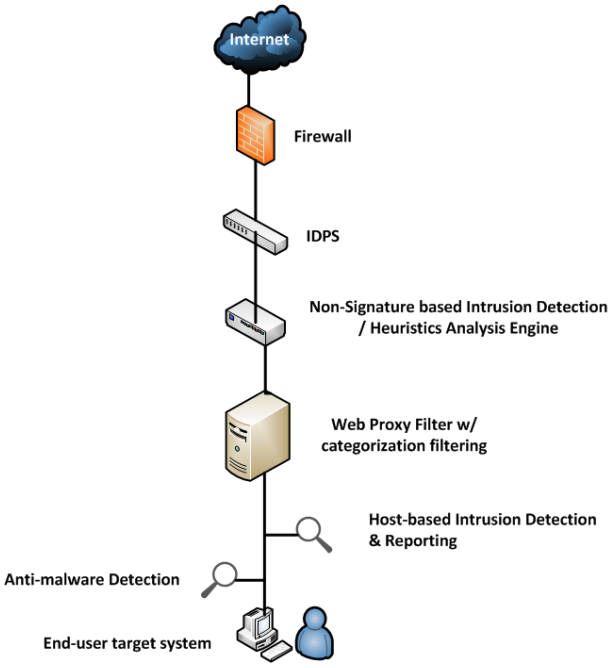
Reaffirmation that a Defense in Depth strategy is key to detection and prevention – A story of Social Media Link-baiting and Malware Targeting

By Ken Foster, Cybersecurity Operations Manager
3/15/2015

A defense in depth strategy is paramount to defending IT resources at the most technically challenging layer of the OSI model to defend, Layer 8 – The Human. The following story helps illustrate my point via a practical example of how infection prevention would likely occur in a well architected Defense in Depth implementation.

According to a recent story by Zeljka Zorz (reference below), a new malicious worm is making the rounds via social media; that isn't news. The tactic of purporting offering scandalous sex photos or other enticing content isn't new; this is the link lure. Since many organizations do not inhibit social media usage via work systems; there is no policy component present to prevent following the link (exception: prohibitions of sexually explicit content which typically receives minor adherence based on SA historical feedback). Certainly the practice of multiple redirects in an effort to fingerprint and custom tailor the malware to the target is a time-tested strategy; nothing new here. So if this scenario is so common, why is it successful? Simple, many of the unwitting victims are not protected via a Defense-in-Depth (D-i-D) strategy.

Let walk the Cyber security stack and see how this attack might have been inhibited or at a minimum detected early in the exploitation phase. Below is a typical medium to large-sized organizations security stack based on a D-i-D strategy:



The key takeaway is layering really works! Consider this exploit from the prospective of a user on a typical workstation in an office environment. For this attack to be successful, the payload must traverse the firewall and perimeter IPS. Both devices are signature-based and looking at the layer 2-3 traffic, not the file and possible payload. We would expect the binary to pass through both of these layers. The first chance of detection would occur on a heuristics-based analytics device monitoring network traffic for binary payloads and there are several vendors in this space. These systems typically detect and detonate the payloads on VM's within the appliance in an attempt to determine if the file is malicious. Let's assume the appliance fails to prevent the payload from infecting the target (possible in highly advanced malware that incorporate VM detection). The next opportunity would be at the target systems Host-based Intrusion Detection/Prevention solution. These solutions look for anomalous system calls in an effort to detect Indicators of Compromise (IoC), inhibit the system call, and alert the security administrator of suspect behaviors. For the sake of argument, let's pose that a long-running timer is present that prevents malicious system calls, allowing the binary makes it to the target system. Just prior to writing the binary to the system, the Anti-malware software resident on the system would hash the file against its known signatures. This signature-based solution also monitors for signs of malware infection. In the case of this malware in the article, Virus-total indicates that 33 / 57 AV vendors currently detect the malware; likely it would have been detected upon delivery to the system's drive.

The point of this walk-through is while Defense-in-Depth is expensive to implement and maintain, it works! This examples identifies 4 possible phases in which the malware could be detected. Organizations must embrace that in a cyber-world of increased volatility, hacktivism, and Advanced Persistent Threat (APT) dejour, the long-running operational costs associated with an effective defense strategy will pale in comparison to the long-term impacts to confidence and trust experienced by those companies who opt to buy insurance and hope firewalls, and Anti-virus are sufficient. Organizations that take this cost-based approach tend to understand and properly perform the required calculus that factors crisis management, remediation manpower, post-incident support, and replacement hardware (in some cases) as part of the total cost calculation.

Image URL: http://www.net-security.org/images/articles/worm-malwarebytes-13032015.jpg

Original Story: http://www.net-security.org/malware_news.php?id=2990

Virustotal Detection Rates:
https://www.virustotal.com/en/file/66973c39d0babe54392cea08c20438dbe70c15602ed9c25a644df6a1d17a06e2/analysis/