



<http://www.itwire.com/cloud-computing/51169-palo-alto-networks-finds-hundreds-of-malware-samples-unknown-to-security-researchers>

Palo Alto Networks finds hundreds of malware samples unknown to security researchers

[David Heath](#)

Wednesday, 16 November 2011 20:02

As part of a typical sales engagement, Palo Alto Networks will place one of their next-generation firewalls onto a potential customer's network to determine 'what's going on.' Turns out, rather a lot.

Palo Alto Networks' recently launched Wildfire malware analysis engine is a cloud-based service that is able to check for malware in any files that are intended to be downloaded via various on-line repository services or email. This is achieved by interaction with their in-line firewall which passes the files to the cloud service for analysis. In return, the cloud system communicates updated signatures to all firewalls at customer sites.

What the company [found](#) was that 7% of all such files destined for corporate users contained some form of malware.

Even more surprising was that a significant portion of the malware was previously unknown to security researchers.

"I think we were all a bit surprised by the volume and frequency with which we were finding unknown malware in live networks," said Wade Williamson, Senior Security Analyst at Palo Alto Networks.

"Unknown malware often represents the leading edge of an organized attack, so this data really underscores the importance of getting new anti-malware technologies out of the lab and into the hands of IT teams who are on the front lines. The ability to detect, remediate and investigate unknown malware needs to become a practical part of a threat prevention strategy in the same way that IPS and URL filtering are used today."

In the previous three months, over 700 unique malware examples were detected, of which 57% were unknown at the time of discovery to either [Virus Total](#) or the various anti-virus vendors. Further, 15% of the newly discovered malware generated what appeared to be malicious or unknown outbound traffic to command-and-control servers.

Of interest was the wider view that Wildfire was able to take. Using the tool, the company was able to

identify specific phishing campaigns based on the unique communication channels; for instance, Palo Alto Networks was able to identify one attacker who almost exclusively made use of AOL Mail and another who hosted his malware laden files at the Hotfile hosting service.