

The MITRE Corporation

License Opportunities



MITRE technology transfer office

MITRE's Technology Transfer program was established in 1999 to place MITRE-developed technologies in the hands of commercial companies that can make them available to our sponsors and the public as supported, affordable products. Working on critical issues of national importance, MITRE continues to develop new and innovative technologies.

The MITRE Corporation
Technology Transfer Office
7515 Colshire Drive
McLean, VA 22102-7539

Phone: 703-983-6053
www.mitre.org/work/tech_transfer/
Email: techtransfer@mitre.org

MITRE

www.mitre.org

HoneyClient

A honeyclient is a virtual machine designed to drive a target application to navigate the Web, hunting for malicious websites that contain or distribute potential malware. To detect potentially malicious software and servers, honeyclients analyze websites, evaluate them against the baseline performance of safe sites, and report their findings about suspect sites and servers to analysts. They can also proactively detect exploits against client applications without known signatures.

MITRE currently operates multiple autonomous honeyclients, which navigate the Web in a spider-like fashion as they hunt for potentially malicious servers, and report their findings about suspect sites and servers back to MITRE for analysis. Together, MITRE's honeyclients search 150 to 300 Uniform Resource Locators (URLs) per hour and approximately 200,000 unique URLs each day. Using a distributed honeyclient system like MITRE's, which allows individual clients to report back to a central repository and to process additional incoming data, increases the effectiveness of honeyclients.

Applications

Many end users and organizations could benefit from using MITRE's honeyclient technology, including service providers. An organization could use MITRE's technology to protect its systems and network from malware and the possibility of low-scale or large-scale attacks. It could also be used to identify malicious sites in a timely manner and to enhance an organization's threat report and advanced warning capabilities.

MITRE's honeyclient technology consists of core software, which is available on MITRE's website as open source code, and an Outlook-based plug-in to collect malicious URLs. To operate a service based on MITRE's open source software, potential licensees must obtain a license based on MITRE's copyrighted open source code. As part of the license agreement, MITRE would provide additional non-open source components and documentation.

Benefits

MITRE's honeyclient technology can be used to protect an organization's systems and network from malware and malicious attacks. By identifying malicious sites and potentially compromising behavior in a timely manner, the technology can be used to enhance an organization's threat report and advanced warning capabilities as well as to create its own line of defense against similar types of attacks.

Additional Information and Links

MITRE's Honeyclient Project: www.honeyclient.org/trac
<http://freshmeat.net/projects/honeyclient/>

Lee, M. "Honeyclients Root Out Attackers' Domains," August 2007, The MITRE Corporation. www.mitre.org/news/digest/advanced_research/08_07/a_honeyclient.html