



ThreatExpert

The Threat landscape is changing, but your need to quickly assess and mitigate your risk has not!

Everyone has heard that the growth of new threats on the internet is ever increasing. New threats are found daily, and with the growth of server side polymorphism, new several variants can be released per minute. Targeted attacks are also on the rise meaning that the threat you find in your environment may be the only one of its kind, or one of a handful in the world.

Given the onslaught of new threats, and constrained by the limits of manual analysis, it could be days or weeks before your AV vendor can obtain a sample, perform an evaluation of your threat, and release a signature update. System Administrators need to bridge that gap.

What is Threat Expert and how does it work?

ThreatExpert is an advanced Automated Threat Analysis System (ATAS) designed to analyze and report the behavior of computer viruses, worms, trojans, adware, spyware, and other security-related risks in a fully automated mode.

ThreatExpert takes a threat file, places it in a self-contained simulated virtual environment, deliberately executes the threat in this environment and then monitors its behavior.

An analogy to ThreatExpert is that of a 'sting operation' set up by a law enforcement organization to catch a criminal suspect in the act of a specific crime. In successful sting operations, the suspect commits the crime under deception, allowing the law enforcement organization to monitor their very movements and determine if they are the culprit.

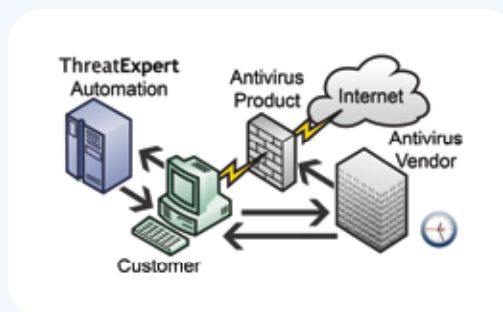
It only takes 2-3 minutes for an automation server to process a single threat, making it possible to generate up to 1,000 highly detailed threat descriptions per server, per day.

ThreatExpert in the Enterprise

When infections are detected within an organization's network, it is the role of system administrators to identify the source of the infections and remove them as quickly as possible.

Infected computers on a network can result in severe losses due to communication problems through impaired network and Internet access, and the unauthorized release of confidential information outside the organization.

Traditionally, when new suspected threat files are identified, system administrators can send these files to an Internet security company, such as an anti-virus or anti-malware vendor, for analysis. These companies investigate the threats and sometime later, possibly ranging from a few up to 48 hours later, depending on the complexity of the threat; provide updated database definitions to remove them. By submitting samples to ThreatExpert – the response time is cut down to minutes.



- Being affected with a new threat, the customer submits the sample both to their current Antivirus Vendor and ThreatExpert
- ThreatExpert provides an immediate detailed threat description analysis
- Threat description can be used by the customer to undertake threat mitigation phase (e.g. automated or manual threat removal or prevention) hours before Antivirus Vendor responds



ThreatExpert

What you will find in your ThreatExpert Report

Submission details – Contains information on when the ThreatExpert analysis commenced, the time taken to analyze the threat file and other data on the threat.

Summary of the findings – Lists threat details in an easy to read graphical format:

What's Been Found	Severity Level
Threat characteristics of the Storm worm (aka CME-711/Peacomm/Nuwar/Zhelatin/Tibs). This threat is normally received as an email attachment; it may consist of a rootkit, a peer-to-peer client, and a mass-mailing worm component. To bypass firewalls, its code may be injected and run from the legitimate services.exe process.	██████████
Capability to send out email message(s) with the built-in SMTP client engine.	██████
Searching for email addresses by enumerating files with the certain extensions. This functionality is used by mass-mailers and spam-bots.	██████████
Backdoor functionality: connected remote users are able to perform multiple actions on the compromised system.	██████████
Creates a startup registry entry.	██████
Contains characteristics of an identified security risk.	██████████

Possible Security Risks – Threats are assessed and categorized

Possible Security Risk

Attention! The following threat categories were identified:

Threat Category	Description
	A malicious backdoor trojan that runs in the background and allows remote access to the compromised system
	A network-aware worm that attempts to replicate across the existing network(s)
	A malicious trojan horse or bot that may represent security risk for the compromised system and/or its network environment

File System Modifications – Lists files, hidden files, ADSs and directories that were added/deleted/modified on the file system by the threat.

Memory Modifications – Lists processes, hidden processes, injected memory pages, modules, services, hooks and drivers that were added to or modified in memory by the threat.

Registry Modifications – Lists keys and values, including hidden keys and values that were added/deleted/modified in the Windows Registry by the threat.

Outbound traffic (potentially malicious) – Lists outbound traffic attempts instigated by the threat, with a description.

Heuristics Analysis – Derived from the analysis of the contents of memory and intercepted traffic. Lists the capability to perform specific malicious activities such as the termination security-related processes, details on replication mechanisms, and keylogging.

Other details – Lists a range of other miscellaneous information such as country of origin, ports opened, and other details from a range of Windows API calls made by the threat.

Generated SMTP traffic – Lists details on outbound e-mail traffic, including details on senders, recipients, subject fields, attachments and the body fields of messages

This detailed report is sufficient for a system administrator to utilize in order to minimize the impact of a new threat infecting their network in the shortest possible time, and it can also be used to provide a second opinion on threat analyses that have been conducted by other sources.

Licensing Options

ThreatExpert is available for licensing as either a web based service, or as an in-house server.

Contact Us

info@threatexpert.com