Periodically, a crash report is generated by a malicious exploit that crashes the application it is targeting. Anomalies in crash reports can indicate new zero-day exploits and malware.

We can create exploit fingerprints to search crash reports for evidence of known exploits. These fingerprints, correlated with global cybersecurity intelligence, can be used to detect previously unknown and undiscovered APTs and zero-day attacks.

100% of Windows PCs send crash reports to Microsoft. Billions of these reports are sent every year.

Windows Error Reporting (AKA, Dr. Watson) creates detailed reports every time an application crashes, then sends the reports out unencrypted to Microsoft. In an industry first, Websense® Security Labs™ researchers used such crash reports to detect unknown threats.

© 2014 Websense, Inc. All rights reserved. Websense, TRITON and the Websense logo are registered trademarks of Websense, Inc. in the United States and various countries. All other trademarks are the properties of their respective owners.

// SOURCE 2014: Websense® Security Labs™
// VISIT: http://securitylabs.websense.com