Cerberus

Cerberus reduces the level of expertise required to perform malware analysis, allowing first and second responders to triage malware and determine behavior and intent without waiting for a malware team. Now actionable intelligence can be achieved before sending malware on for deeper analysis.

Cerberus Malware Analysis is Part of the CIRT Integrated Response Platform.

Using CIRT You Can…

- Scan computers across the enterprise for executables.
- Suspect binaries identified through host analysis are automatically given a threat score.
- Set a threat score threshold: IF threat ≥ 40 THEN automatically initiate stage two.
- Basic and advanced disassembly extracts arguments to determine what the binary is capable of doing.
- Verify behavior and intent by correlating data with host and network analysis.
- Remediate and have CIRT monitor for new and recurring threats.

What is Cerberus?

Cerberus is a malware triage technology that is incorporated into AccessData's integrated incident response platform, CIRT (Cyber Intelligence & Response Technology). It is also available as an add-on for FTK 4. The first step towards automated reverse engineering, Cerberus provides threat scores and disassembly analysis to determine both the behavior and intent of suspect binaries.

Cerberus Works in Two Stages…

Stage 1

During Stage 1 analysis, Cerberus tallies attributes of each binary to generate threat scores that approximate how "dangerous" each binary might be.

Stage 1 looks for characteristics that are immediately apparent, such as "does this binary contain a valid digital signature?", "is this binary packed?", and "what OS functions does this binary import?" Therefore the Cerberus Stage 1 analysis is extremely fast and can be run against a large number of binaries quickly.

Stage 2

Stage 2 analysis is much more complex, as it disassembles the entire binary, develops an understanding of the binary code flow, and outputs a list of operating system functions that are called by the binary, along with the arguments that are passed into those functions. Additional analysis provides details such as function arguments, which could reveal things, such as Internet callback addresses, file names and other statically compiled artifacts.

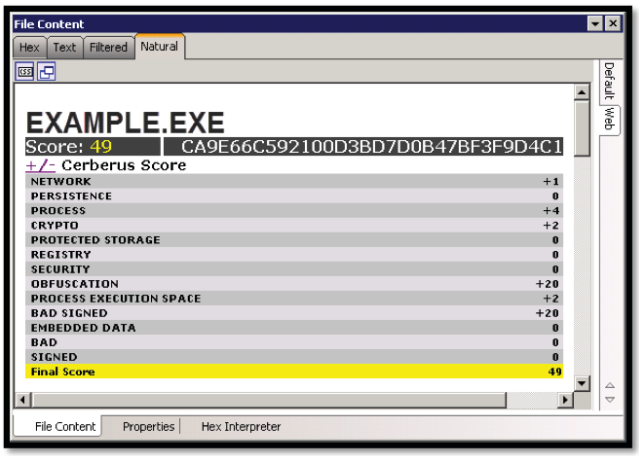
Cerberus Malware Triage vs. Traditional Malware Analysis…

Triaging potential malware with Cerberus gives first and second responders immediate actionable intelligence without waiting for a malware team to spend days or even weeks employing traditional methods of analysis. The Cerberus feature in CIRT provides response teams with critical threat information that they can then correlate and verify with CIRT's network and host analysis.

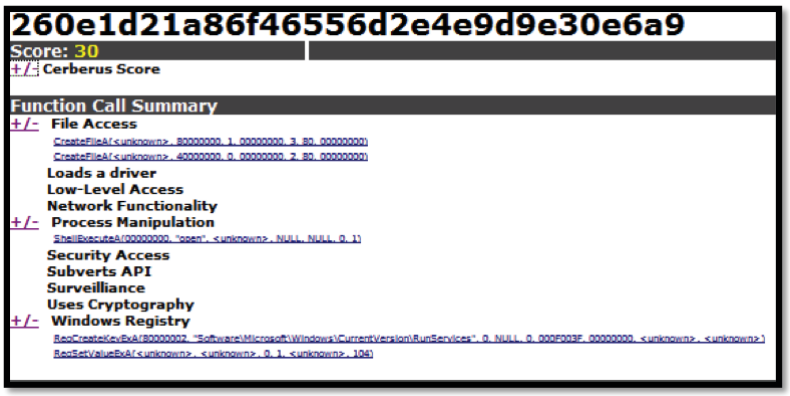
Furthermore, while deeper examination is often needed in the event of a security incident, these traditional methods each have its own shortcomings, which Cerberus methodologies avoid.

- **Dynamic Analysis** is often not reliable, because the binary could recognize that it is being analyzed and perform a different action in order to intentionally fool the analyst.
- **Traditional Heuristics** are not based on the fundamental characteristics of malware and have high false positive / false negative rates.
- **Signature-based / Byte String Analysis** cannot detect new malware or new variants and requires prior knowledge in the form of an action or byte string.

AccessData®



STAGE 1:
Identify binaries with unusually high threat scores and view attributes contributing to those scores.



STAGE 2:
View capabilities of binary in predefined categories along with arguments.

AccessData®

Contact Us:

NORTH AMERICA SALES
800.574.5199
801.765.4370 (fax)
sales@accessdata.com

INTERNATIONAL SALES
Office: +44 (0)20 7010 7800
internationalsales@accessdata.com