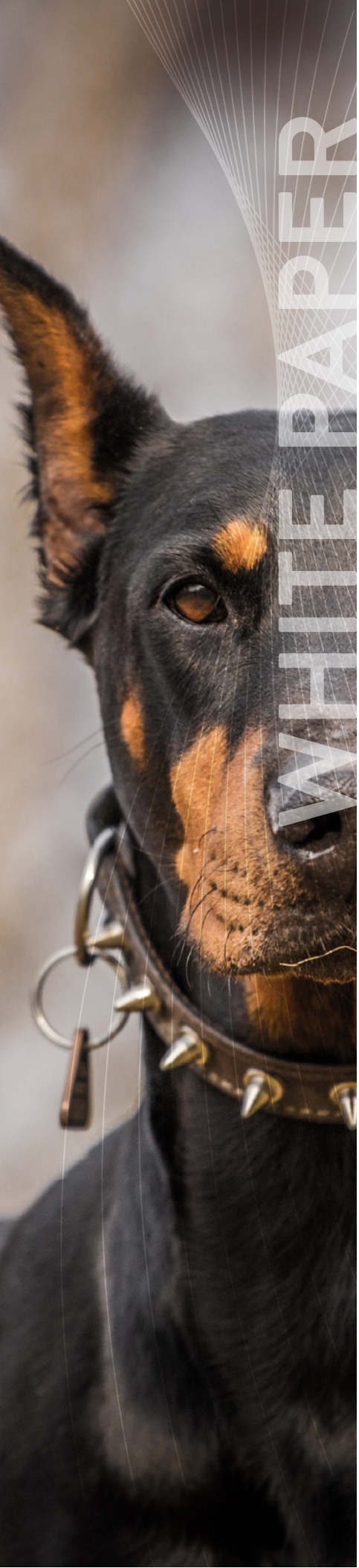


ACCESSDATA

Protect yourself: How Cerberus blocks malware and viruses in an investigation

Organizations around the world are exposing themselves and their entire network to potential risk every day.

How is this happening?

Infecting Your Own System

Imagine this: A laptop, computer or other electronic device has been seized to see if it contains data that's relevant to your case. The examiner images the machine, not knowing what type of viruses or malicious code might be lurking on the imaged drive. As required, the investigator images the drives—and accidentally picks up malicious files along with the data they need.

While most computer forensic tools, including Forensic Toolkit®, insulate the users' machine and network from exposure and infection from malicious code, sometimes the user needs to export a file to their desktop and view it in its native state. For example, once the file is exported, all insulation is gone and the examiner's network is exposed to what's in the Word document, where cyber criminals attempt to hide malware.

It's the first layer of defense against the risk of imaging unknown devices and allows you to identify risky files after processing your data in FTK®. Then you can see which files are infected and can avoid exporting them.

Users may inadvertently infect their computer with ransomware, Trojan or any other form of malware aimed at holding the data hostage or flat out stealing the data.

This could easily happen to you. Your document may have been quarantined inside of FTK, so your network and personal assets were protected, but since you exported the file to the desktop, you released the malware.

What's the Solution?

Since these threats are common today, IT, litigation support and examiners need to protect their assets and mitigate risk.

Cerberus can help. You can enable this fully integrated malware analysis tool within FTK simply by activating the Cerberus license. It's the first layer of defense against the risk of imaging unknown devices and allows you to identify risky files after processing your data in FTK. Then you can see which files are infected and can avoid exporting them. Cerberus helps you identify malicious files and helps you answer these and other questions:

1. When does the file run—at startup, or when other services are activated?
2. What ports is it attempting to communicate through?
3. Is it communicating back to the website or other server out of your network?

The Workflow

Let's start with a sample case.

You're sitting in the lab with FTK and have the case built up on the computer but no data loaded in. IT brings in a hard drive so you can process evidence.

Here are the best first steps:

- **Load the potentially contaminated data into FTK.** If you have the Cerberus license, you will easily be able to see the files that you do not want to export to your hard drive.
- **If you don't have Cerberus**, when you click on a document and can't view it in its native format, don't right-click and select export, or click export and open with a program. This unleashes the potentially contaminated document.
- **If you have Cerberus:** Go into Evidence, Additional Analysis, and run a Cerberus processing job. Leave the Cerberus option to default, and run on all items.

During these steps, you'll notice Cerberus has two layers.

- **Stage 1—Threat Analysis:** Determines when the program runs and whether it's potentially bad.
- **Stage 2—Static Analysis:** Goes deeper to find the binary 1s and 0s so an examiner can report what's bad and why.

Apply the Cerberus Score Filter

The Cerberus Score filter allows you look at only the documents that have been analyzed for malware and viruses and assigned a threat-level score. In the Cerberus Score column you'll be able to know which ones to stay away from.

The scores are in pluses and minuses. The higher the score, the bigger the threat. The lower the score, even into the negatives, the less the threat.

- If the score is over 100, it's a red flag that the document has a high probability of malware.
- Any score over 50 is something to be skeptical about.

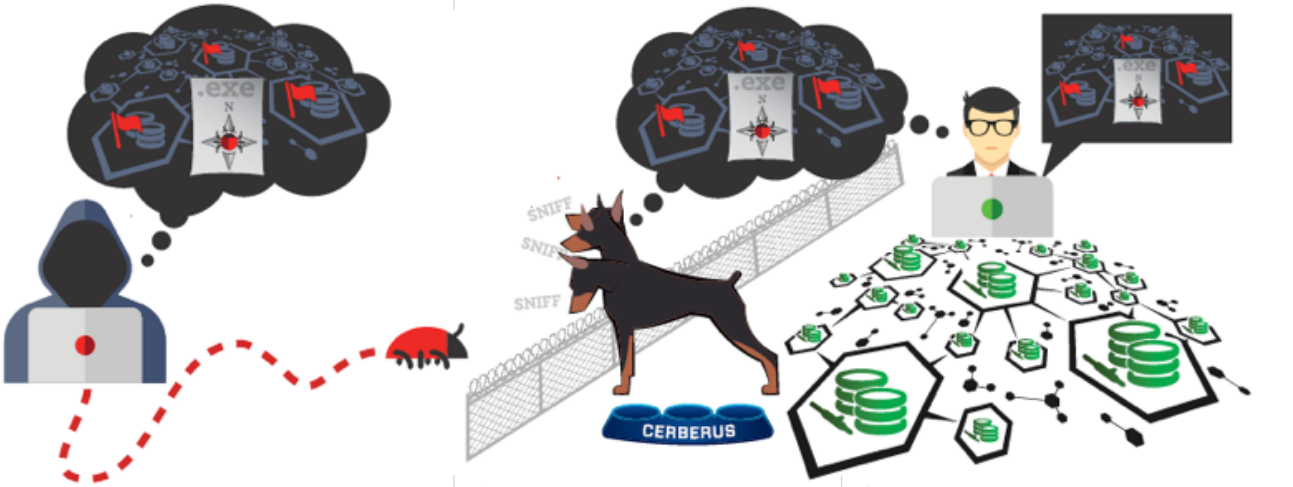
This scoring also gives insight into medium and low risk items.

For a deeper analysis, the Cerberus Static Analysis shows only the items that have had Cerberus Static Analysis run against them in the dialog box. You can view a threat score report for each executable file, showing the score that was calculated during processing. The report also shows general file properties.

How Cerberus Works

1
Criminal creates a virus and arms it with an executable.

2
Executable comes into contact with Cerberus.



3
Cerberus is able to sniff out the malicious intent of the malware by emulating all the paths throughout the executable.

In other words, Cerberus is letting the malware think it's calling the shots, while in reality, Cerberus is exposing the malware to even closer scrutiny.

By emulating the instructions internally, an analyst need not worry about malicious executables invading their machine because of vulnerabilities in the sandbox environment.

4
Cerberus communicates the malware's plan of attack and capabilities to its owner instead of merely reporting what it did during a few executions. Cerberus' instinctual analysis of the situation allows its owner to quickly identify threats while not wasting time with benign files.

Since malware can usually detect that it's running in a sandbox, the heightened awareness of Cerberus is essential for triaging an executable that has malicious intent.

Conclusion

Cerberus lets you know what is safe to open outside of FTK, allowing users to see malicious files and protect their assets from malware and viruses on their systems.

For more information about Cerberus and other forensic solutions, contact an AccessData Representative today.

AccessData Group has pioneered digital forensics and e-discovery software development for more than 25 years. Over that time, the company has grown to provide both stand-alone and enterprise-class solutions that can synergistically work together to enable both criminal and civil e-discovery of any kind, including digital investigations, computer forensics, legal review, compliance, auditing and information assurance. More than 130,000 customers in law enforcement, government agencies, corporations and law firms around the world rely on AccessData® software solutions, and its premier digital investigations products and services. AccessData Group is also a leading provider of digital forensics training and certification, with its AccessData Certified Examiner® (ACE®) and Mobile Phone Examiner Certification AME programs. For more information, please go to www.accessdata.com.

Global Headquarters
+1 801 377 5410
588 West 300 South
Lindon, Utah

North American Sales
+1 800 574 5199
Fax: +1 801 765 4370
sales@accessdata.com

International Sales
+44 20 7010 7800
internationalsales@accessdata.com

LEARN MORE

www.AccessData.com