SONICWALL®

WHY RETAIL NETWORKS NEED REAL-TIME DEEP MEMORY INSPECTION

How SonicWall Real-Time Deep Memory Inspection™ improves retailers' protection against malware and ransomware.

Abstract

In 2017, the retail industry was the No. 1 target of cyberattacks.[1] Retailers face multi-vector attacks using malicious code that is more and more difficult to detect before it detonates. SonicWall's patent-pending Real-Time Deep Memory Inspection™ (RTDMI) technology, a recently-developed engine for the Capture Advanced Threat Protection (ATP) service, adds a new depth of protection against malware at no additional cost to Capture ATP customers.

Retail and ransomware

Of all the different types of cyberattacks, ransomware is particularly problematic for the retail industry. Malware, which encrypts files, systems, or even entire networks, like WannaCry, puts a stop to operations in stores and to online ecommerce immediately. Ransomware doesn't just impact your immediate revenue streams; it can significantly reduce consumers' confidence in your business and drive many customers to your competitors.

[1] *"Retail sector top cyber attack target" Warwick Ashford, Computer Weekly, April 5, 2018*

Your point-of-sale systems (POS), particularly the newer tablet-based platforms, are particularly vulnerable. The key target of hacked POS systems is the cardholder data they contain. That cardholder data is money in the bank for cybercriminals. For retailers whose POS systems are breached, it's money out of the bank; revenue and customers lost, not to mention potential PCI compliance issues.

Capture ATP and the RTDMI engine can detect and block new, zero-day and targeted malware (including ransomware), to a significantly higher degree than other available solutions.

Capture ATP: A more effective sandbox

Typical network sandboxes are isolated environments in which suspect files can be executed, after which sandbox engines examine the results for malicious behavior. These sandboxes are not without their own limitations; they can generate both false convictions and false acquittals, and degrade the end-user experience.

These limitations have become more problematic as malware writers continue to develop more complex and sophisticated attack techniques. Custom encryption, packing and deeper obfuscation — even sensing that the code is being deployed in a sandbox — techniques can hide malware from the static detection techniques employed by most single-engine sandboxes.

SonicWall Capture ATP was the first multi-engine sandbox able to block files at the gateway until a verdict. Using multiple sandbox engines, executing in parallel, increases the likelihood of detecting malware by its effects from the application level down to actual hardware-level code.

The development and deployment of the RTDMI engine demonstrably improves the effectiveness of Capture ATP against even the most obfuscated malicious code. RTDMI adds a layer of protection against malware that eludes other detection methods.

How RTDMI works

RTDMI forces malware to reveal itself. In its secure sandbox environment, it de-obfuscates code that has been obfuscated to avoid detection. Once de-obfuscated in the sandbox memory, the code executes, and RTDMI detects the malicious code before it impacts system behavior. That is a key advantage of RTDMI over other analysis techniques that attempt to differentiate between normal and malware-triggered system behavior.

RTDMI looks at the suspect code and compares it to other code sequences it has already seen, using machine learning. Due to the engine's execution speed, it can identify malicious code in less than 100 nanoseconds, resulting in an extremely fast verdict.

SonicWall Capture Labs has verified that the RTDMI engine can stop new forms of malware that attempt to exploit the Meltdown and Spectre vulnerability. The engine can detect issues down to the level of actual CPU instructions, unlike behavior-based systems that only reach down to the level of APIs and system calls.

What RTDMI detects

Capture Labs tested RTDMI side-by-side with third-party network sandboxing technologies. Once the RTDMI engine was implemented, it detected hundreds of new forms of malware embedded in PDFs and Microsoft Office files. RTDMI discovered 35 times as many malicious PDF files and nearly twice the amount of malicious Office files than the other engines.

RTDMI inside Capture ATP combines both static inspection and dynamic analysis using proprietary exploit detection technology, so is able to detect:

- Malicious Flash-based Office documents
- Dynamic Data Exchange (DDE) based exploits and malware inside Office files
- Malicious Office and PDF files containing executables
- Malicious PDF files containing Office malware
- Shellcode-based malicious Office and PDF files
- Macro-based malicious Office documents
- Malicious multi-layer PDF and Office documents
- Office and PDF-based malware utilizing dynamic proprietary exploit detection technology
- JavaScript-based exploits in PDF documents
- PDF documents containing "JavaScript infectors"
- "Phishing style" malicious PDF documents leading to both phishing and malware hosting websites

These cyberattack methodologies are pertinent to retailers. Office files, such as Word documents and Excel spreadsheets, as well as PDF documents, are part of retailers' daily business operations.

RTDMI in action

The SonicWall on-demand webcast "Identify and Stop Malware in the Quickest and Most Accurate Way Possible," presents two examples of how the RTDMI engine has elevated Capture ATP to new levels of malware detection.

Example 1: The case of the RAT

The first example involves a Remote Access Trojan (RAT), key to numerous forms of info stealers. A Trojan can take control of a system, capture keystrokes, even turn on webcams and microphones without the user's knowledge. It gathers information that can be used to blackmail an individual or a business, encrypt files or lock up retail systems until a ransom is paid.

One recently-developed RAT was encapsulated within an Office document. The document was delivered by email. The document included an attachment, purportedly an invoice, and advised the victim to open the attachment (olepackage.doc) to view the invoice. That attachment was the delivery mechanism for the RAT.

At the time of the detection, the existence of the RAT file was not listed on popular malware search portals. In Capture ATP, it went through the verdict check. It went through the community check of over 60 different virus scanners.

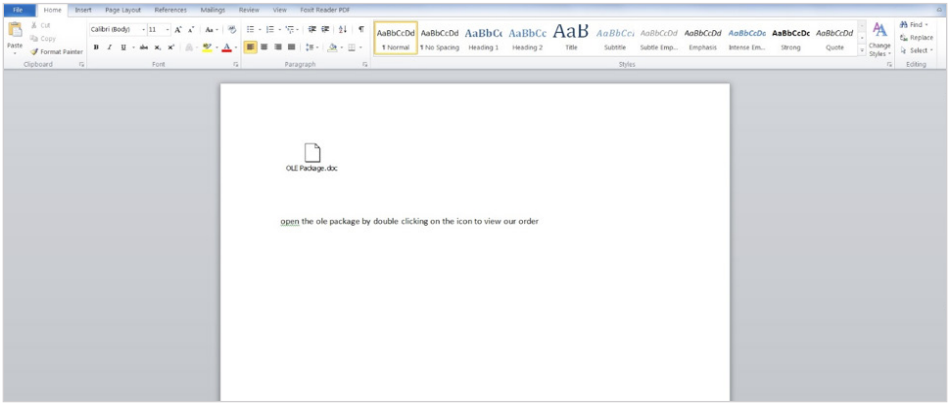

Figure 1 - The embedded file contains the malware

Nothing was seen, so it had to go through dynamic processing.

Of the three engines running in Capture during processing, two of them couldn't find any problems with the code. However, the third RTDMI engine successfully identified the code as being malicious.

If the targeted system had a Java runtime installed, upon opening this RAT file, it executed and revealed its malicious behavior. The RAT file drops a copy of itself into the system's %temp% folder, drops a VBScript file, and downloaded and executed password recovery and other spying tools. It then modified the Windows registry to disable existing installed antivirus and security software, as well as disabling System Restore from the registry.

Here is the Capture ATP report showing the detection of the RAT file by the RTDMI engine:

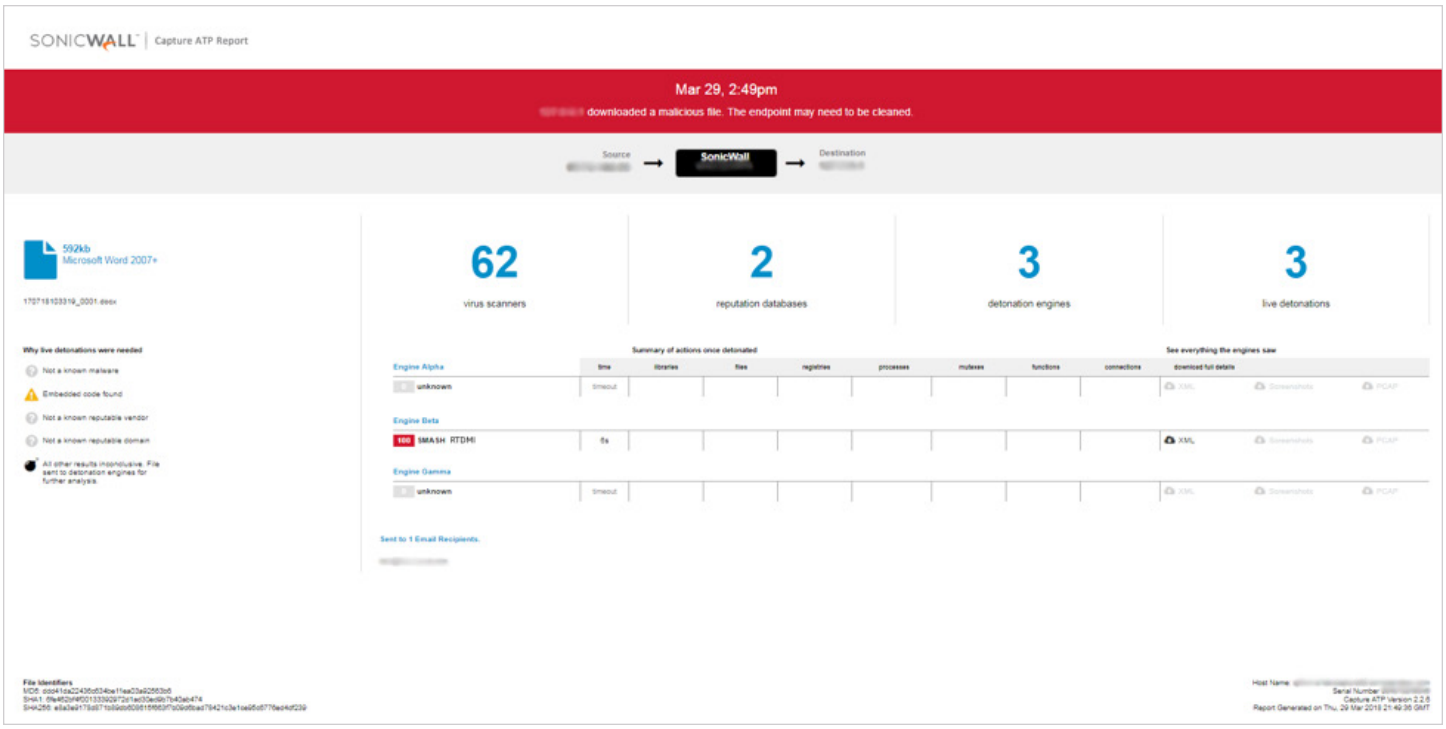

Figure 2 - RTDMI caught the RAT.

Example 2: Cerber, Cerber everywhere

Cerber ransomware encrypts files, and then demands payment before it decrypts and gives the files back to the owner. It's a particularly active form of ransomware, often delivered by email that has an infected Office document as an attachment. Anyone can buy Cerber in exchange for a cut of the profits.

Capture ATP and the RTDMI engine are well familiar with and well able to detect and block Cerber.

Recently, on one device, Capture ATP found 500 new forms of malware a day, and Cerber ransomware twice a day. This is because Cerber is being put into exploit kits and modified, so that its signature is different. That is why signatures do not work against the newest threats. Cerber attempts to get around network security, Windows Defender and other countermeasures to get into systems and wreak havoc. In this example, it had applied seven different evasion tactics, including keyboard layout and putting in timing delays.

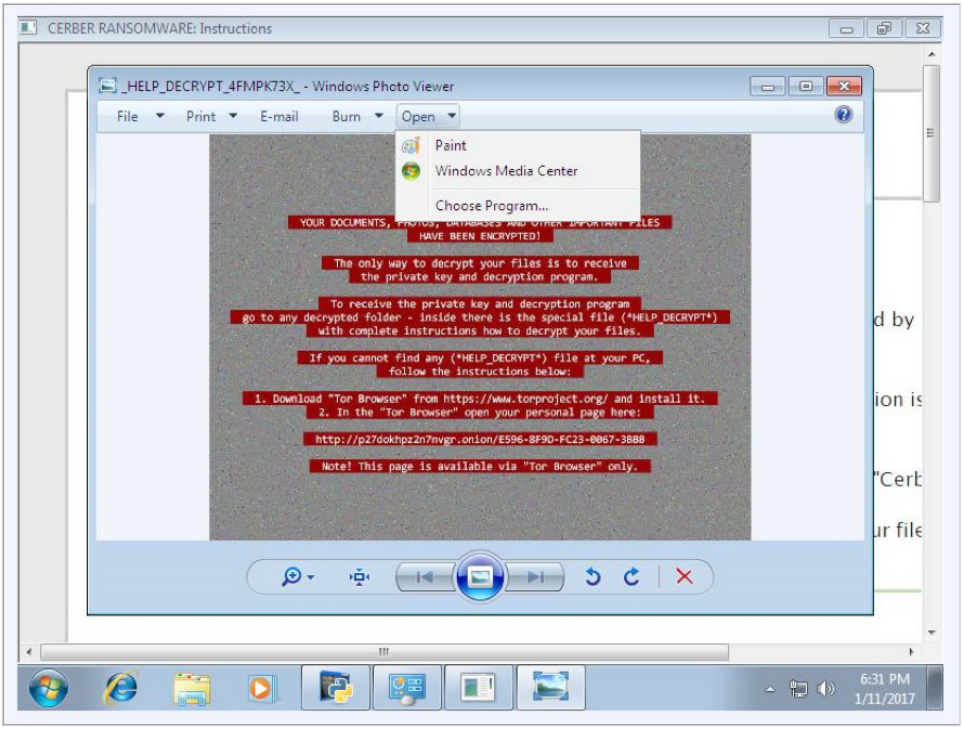

Figure 3 - Cerber in action.

To counter these mutating threats, Capture ATP technology extrapolates what the code wants to do to the application, down to the operating system, down to the software that resides on the hardware. Capture ATP can view an XML file, and examine all the different things that the malware wants to do. This is how Capture ATP came to the verdict that this is malicious.

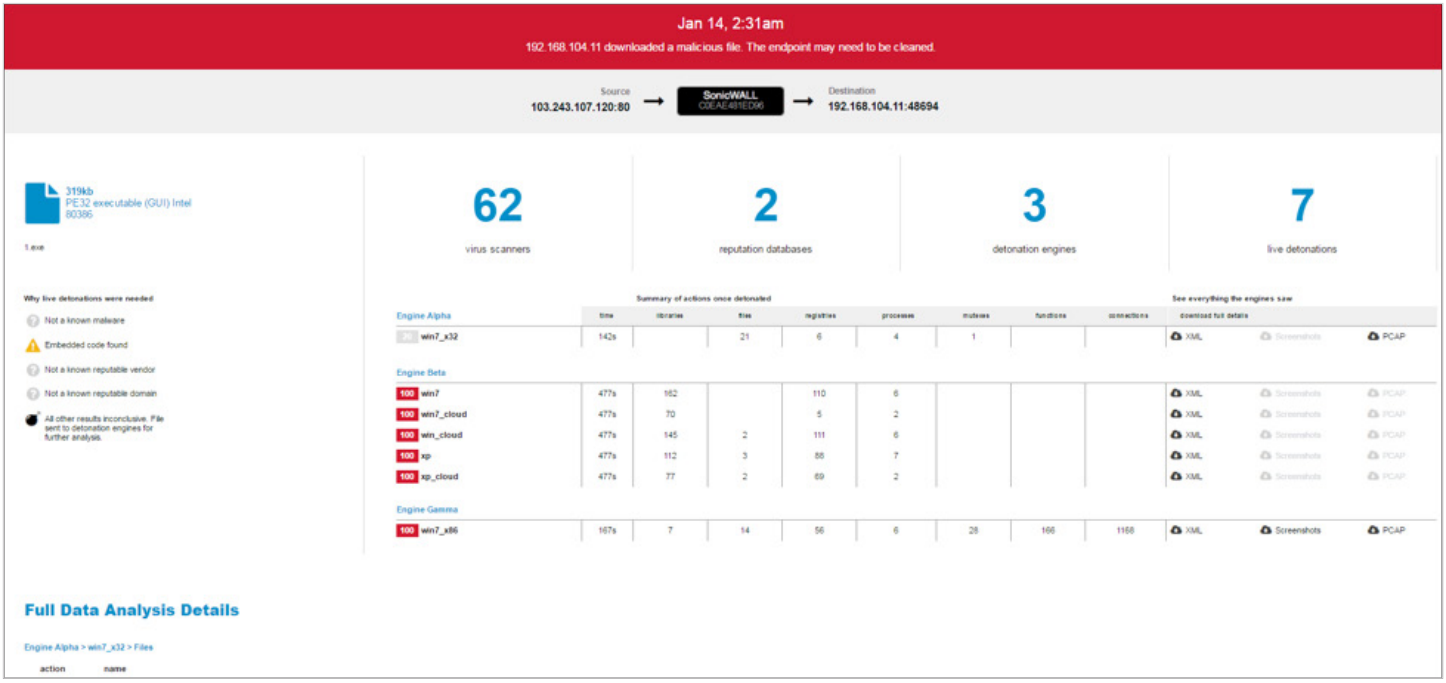

Figure 4 - Capture ATP with RTDMI detects and stops Cerber ransomware

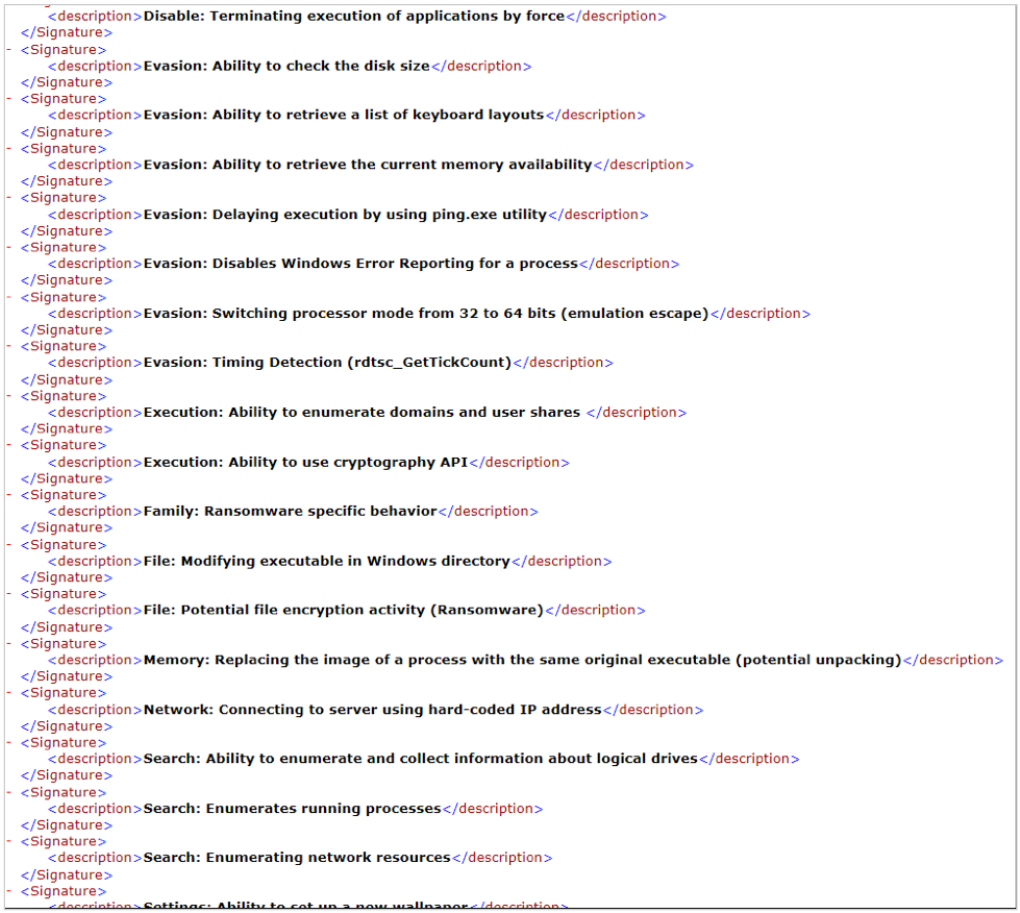

Figure 5 - Inside the Cerber XML file

Conclusion

The enhancement of Capture ATP to islolate, understand, and block malware through the RTDMI engine is a significant breakthrough, and represents increased protection of retailers' revenue, operations, and reputation. SonicWall identified more than **49,800 new attack variants** in the first quarter of 2018, with its new RTDMI technology identifying **5,000 never-before-seen variants**.

SonicWall RTDMI and Capture ATP are the protection retailers need from malware, ransomware, and any cyberattacks that are aimed at them.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com