



Copyright © 2019 FireEye, Inc. All rights reserved.  
Privacy & Cookies Policy | Privacy Shield | Legal Documentation

Site Language  
English

# SMB Exploited: WannaCry Use of "EternalBlue"

May 26, 2017 | by [Ali Islam](#), [Nicole Oppenheim](#), [Winny Thomas](#)

**EXPLOIT**   **MALWARE**   **SMB**   **WANNACRY RANSOMWARE**

Server Message Block (SMB) is the transport protocol used by Windows machines for a wide variety of purposes such as file sharing, printer sharing, and access to remote Windows services. SMB operates over TCP ports 139 and 445. In April 2017, Shadow Brokers released an SMB vulnerability named "EternalBlue," which was part of the [Microsoft security bulletin MS17-010](#).

The recent [WannaCry ransomware](#) takes advantage of this vulnerability to compromise Windows machines, load malware, and propagate to other machines in a network. The attack uses SMB version 1 and TCP port 445 to propagate.

## Context

SMB provides support for what are known as SMB Transactions. Using SMB Transactions enables atomic read and write to be performed between an SMB client and server. If the message request is greater than the SMB MaxBufferSize, the remaining messages are sent as Secondary Trans2 requests. This vulnerability affects the srv2.sys kernel driver and is triggered by malformed Secondary Trans2 requests.

## Working

After the initial SMB handshake, which consists of a protocol negotiate request/response and a session setup request/response, the ransomware connects to the IPC\$ share on the remote machine. Another related aspect of this attack is that the malware is configured to connect to a hardcoded local IP, as shown in Figure 1.



Promotion



Recent



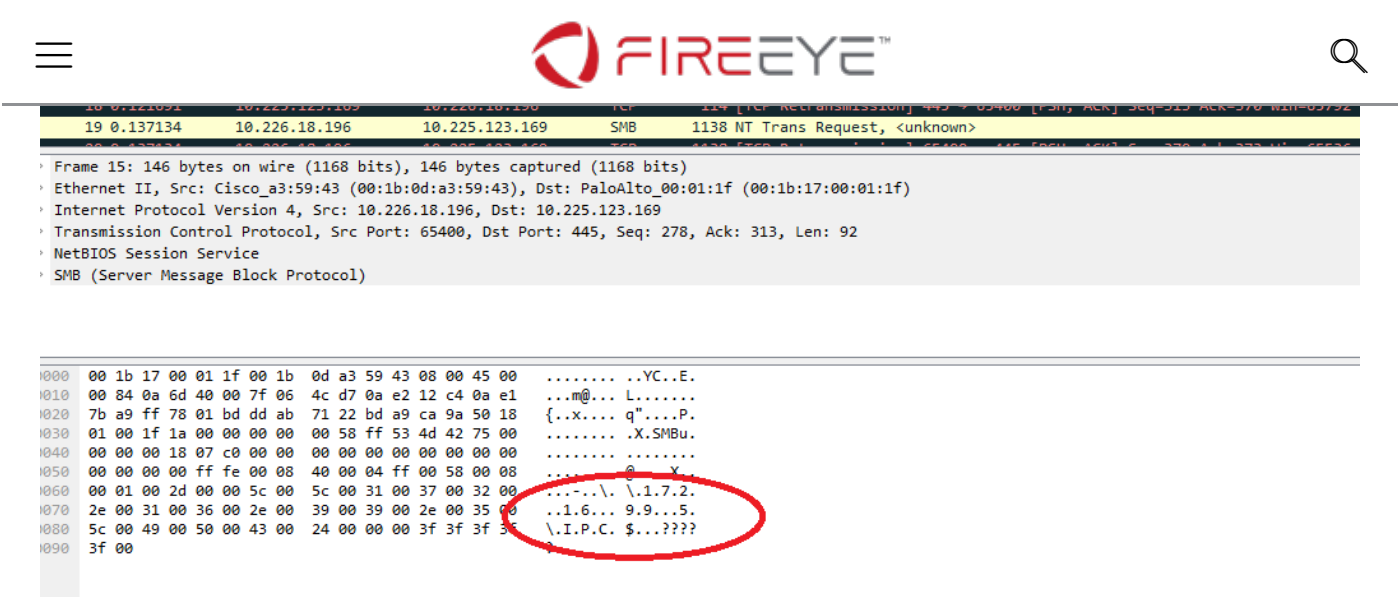
Share



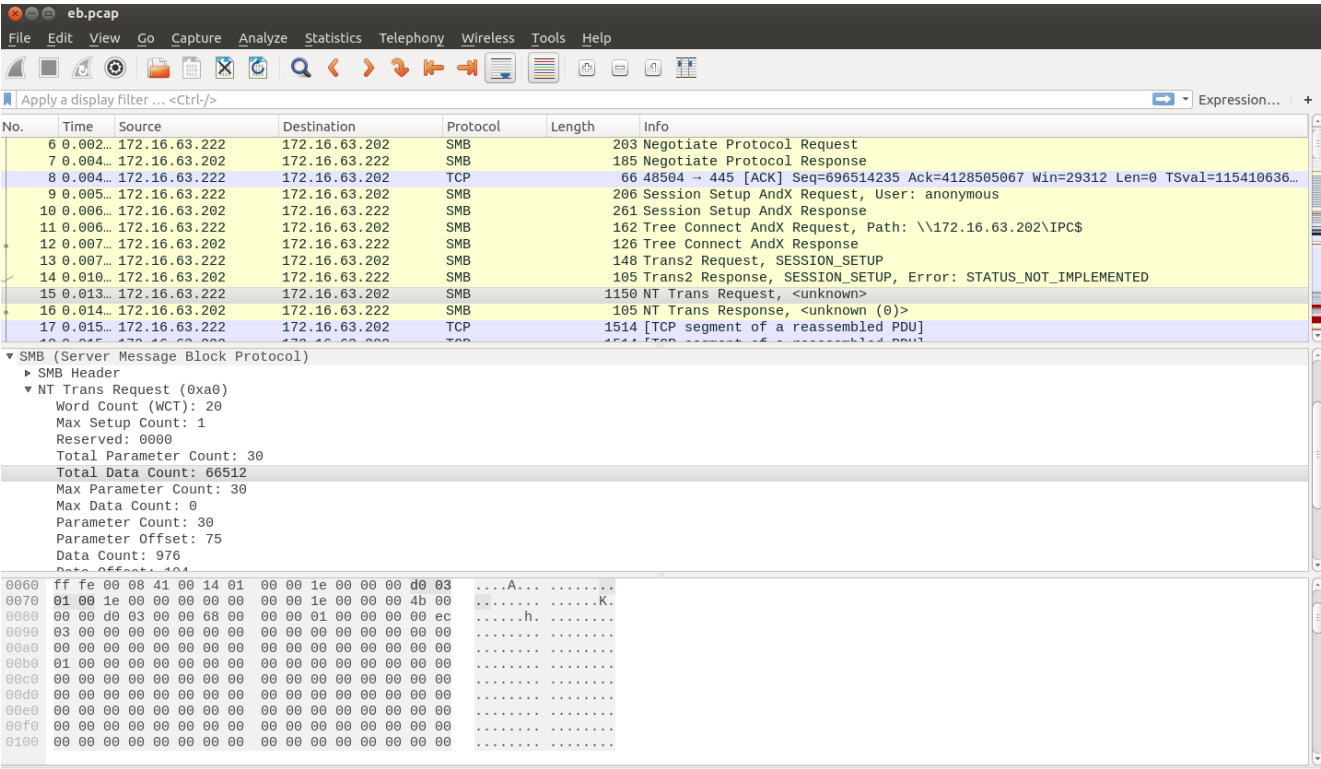
Subscribe



RSS



Next it sends out an initial NT Trans request, which is a huge payload size and consists of a sequence of NOPs, as shown in Figure 2. What it essentially does is move the SMB server state machine to a point where the vulnerability exists so that the attacker can then exploit it using a special crafted packet.



Speaking the SMB language, the large NT Trans request leads to multiple Secondary Trans2 Requests to accommodate for the large request size. These Secondary Trans2 requests are malformed, as seen in the Figure 3. They act as a trigger point for the vulnerability, and the request data portion contains the shellcode

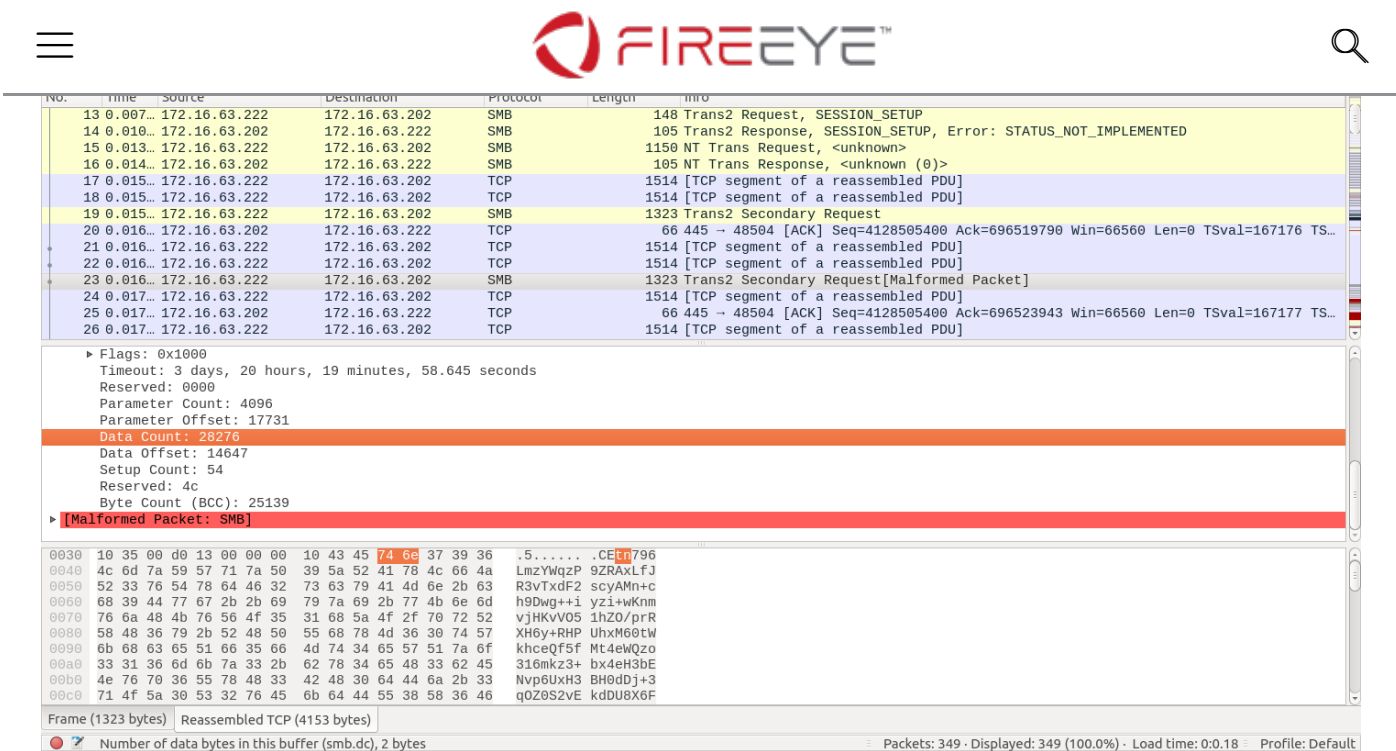


Figure 3: Overflow via Malformed Trans2


## Post Exploitation & Full Cycle

On successfully triggering the vulnerability, an encrypted payload containing the stager for the malware is loaded on the remote machine. The payload delivered to the remote machine launches a service “mssecsvc” from within the lsass process. This service scans the local network and the internet for machines that are accessible and have exposed SMB ports. The service then uses the aforementioned vulnerability to gain access to a remote machine and deliver the malware payload, thus completing the full cycle. All of these activities happen very quickly and the attack penetrates all machines in a typical LAN within minutes.


The ransomware contains two parts, the main executable file containing the code for scanning the network and triggering the SMB vulnerability on accessible machines. Within the resource section of this executable is another executable file embedded in a section named “R”, which contains the ransomware code. The executable containing the ransomware code has an encrypted ZIP file embedded in the resource section named “XIA”. The encrypted ZIP file contains encrypted keys, image files, Tor client and two other executables: taskdl.exe and tasse.exe. The ZIP file contents can be extracted using the password WNCry@2ol7 embedded within the malware code

## Mitigation


There are anomalies and patterns in the NT Trans, Trans2 requests and responses packets that analysts and researchers can use to create useful network level detection. A couple of example signatures that can be deployed are found [here](#) and [here](#).




Promotion




Recent



Share



Subscribe



RSS

Company

Why FireEye?

Customer Stories

Careers

Certifications and Compliance

Investor Relations

Supplier Documents

News and Events

Newsroom

Press Releases

Webinars

Events

Awards and Honors

Email Preferences

Technical Support

Incident?

Report Security Issue

Contact Support

Customer Portal

Communities

Documentation Portal

FireEye Blogs

Threat Research

Solutions and Services

Executive Perspectives

Threat Map

View the Latest Threats

Contact Us

+1 877-347-3393

Stay Connected

Promotion

Recent

Share

Subscribe

RSS

4 of 4

7/2/19, 3:11 PM