THREAT BRIEF

EternalBlue (CVE-2017-0144)

Uncovering a Widely Used Server Message Block Exploit • Winter 2020

Gartner COOL VENDOR 2020™

As part of a purported major leak of the National Security Agency's offensive toolkit, an exploit known as ETERNALBLUE (ETB) surfaced in early 2017. ETB took full advantage of CVE-2017-0144, a vulnerability in the implementation of the Server Message Block (SMB) protocol in Windows 7 and below. A month prior to ETBs release, Microsoft issued a patch for the vulnerability, but public adoption of that patch was slow. The resulting inability to patch throughout 2017 led to several highly effective malware and ransomware campaigns that used ETB as a spreading mechanism; these included WannaCry, NotPetya, and Satan Ransomware.

SMB is an application-layer network protocol providing shared access to files, printers, and serial ports, as well as various communications between nodes on a network. ETB leverages three different bugs found in the SMB protocol implementation of the operating system; those vulnerabilities are summarized as follows and are explicitly controlled by the attacker:

1. A buffer overflow triggered by an incorrect size value in SMB packets
2. A non-compliant SMB transaction sequence which over-allocates memory space
3. A heap-grooming technique designed to write shellcode into the allocated space

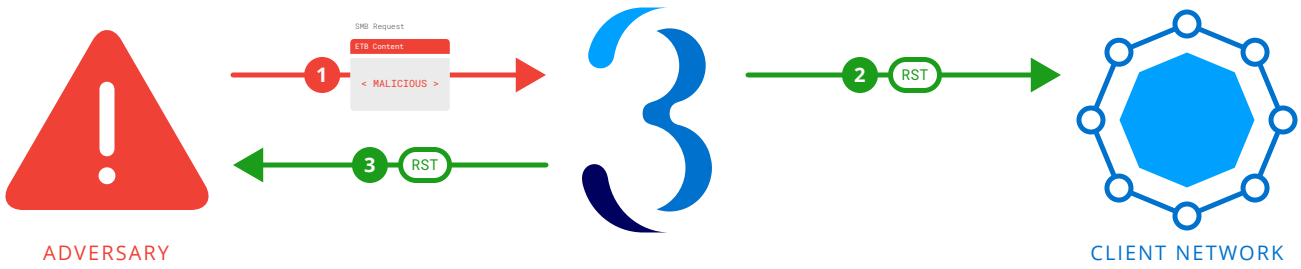
ETB is typically used against a vulnerable target in three stages: scanning, exploitation, and verification. While lesser skilled adversaries, known as "script kiddies," may use all stages of ETB to attack a target, some sophisticated actors can skip the first and last stage entirely.

Stopping All Stages of the Attack

Trinity Cyber detects ETB stages independently—from buffer overflow to heap-groom and implant drop. This approach gives us the ability to act regardless of which stages happen within an SMB session. We support bidirectional, full session detection, which covers ETB attacks regardless of whether they begin as inbound scanning, or outbound exploit traffic designed to infect machines over the open internet.

Once any stage of ETB is detected, our advanced threat prevention service immediately and invisibly closes the malicious session. Our action options also allow us to modify or alter ETB traffic in unique ways to cause additional adversary failure, allowing us to match our client's risk posture.

Trinity Cyber constantly updates our ability to neutralize threats such as ETB. Using our working knowledge of the exploits, we protect our clients from EternalBlue threats regardless of their patching status.



sales@trinitycyber.com • (240) 842-9900 • trinitycyber.com

Trinity Cyber