# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:39:44 UTC



## Tool: EternalRomance

| | |
|---|---|
| Names | EternalRomance |
| Category | Exploits |
| Type | 0-day |
| Description | (Microsoft) ETERNALROMANCE is a remote code execution (RCE) exploit against the legacy SMBv1 file sharing protocol. It takes advantage of CVE-2017-0145, which has been patched with the MS17-010 security bulletin. One might note that file sharing over SMB is normally used only within local networks and that the SMB ports are typically blocked from the internet at the firewall. However, if an attacker has access to a vulnerable endpoint running SMB, the ability to run arbitrary code in kernel context from a remote location is a serious compromise.<br><br>This exploit was written to remotely install and launch an SMB backdoor. At the core of this exploit is a type confusion vulnerability leading to an attacker offset controlled arbitrary heap write. As with almost any heap corruption exploit, the attacker must know or control the layout of the heap to consistently succeed. With SMB, most objects are allocated in the non-paged pool. |
| Information | <https://www.microsoft.com/security/blog/2017/06/16/analysis-of-the-shadow-brokers-release-and-mitigation-with-windows-10-virtualization-based-security/> |
| AlienVault OTX | <https://otx.alienvault.com/browse/pulses?q=tag:eternalromance> |

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

### All groups using tool EternalRomance

| Changed | Name | Country | Observed |
|---|---|---|---|
| **APT groups** | | | |

| | | | | |
|---|---|---|---|---|
| | Calypso |  | 2016-Aug 2021 | |
| | Turla, Waterbug, Venomous Bear |  | 1996-2024 | |

*2 groups listed (2 APT, 0 other, 0 unknown)*

---

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=0ee2c1e7-406f-44af-9fbc-cc45b050f26f