

FireEye

2020 12 8 FireEye Snort Yara ClamAV
OpenIOC GitHub
300 AVL SDK
Red Team CVE
60 304
1
macOS 2 Linux HASH
FireEye Windows
Snort Yara ClamAV OpenIOC / Tools
29
Snort 164 Yara
FireEye 23 ClamAV 88 OpenIOC

FireEye

FireEye

FireEye IEP
PTD PTA
CobaltStrike Metasploit
FireEye
0day ATID
（本文为报告节选，完整报告请扫描下方
CommandoVM HASH 二维码查看）
FireEye

FireEye
Hash Snort Yara ClamAV
OpenIOC

D-Link 3.17 D-Link DSR-150 CVE-2020-25757 CVE-2020-25759
DSR-250 DSR-500 DSR-1000AC VPN CVE-2020-25758 D-Link
Digital Defense
root LAN / WAN
Digital Defense
3.14 crontab