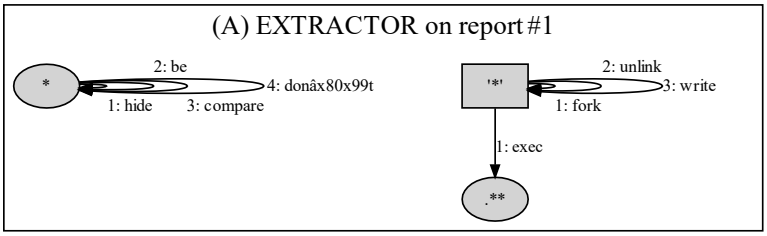

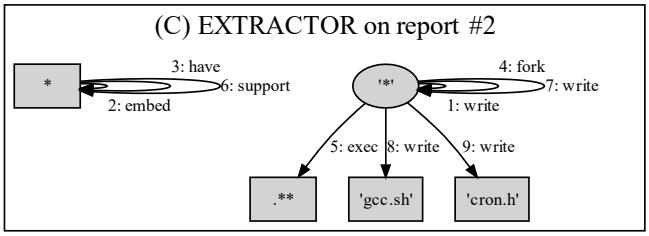

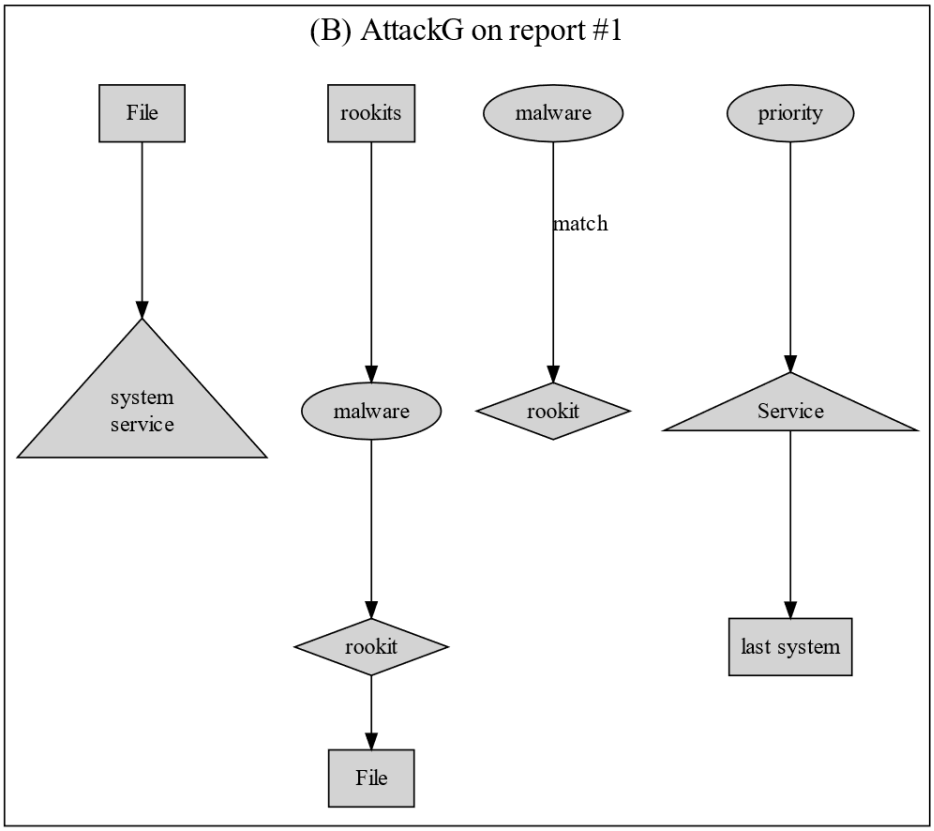

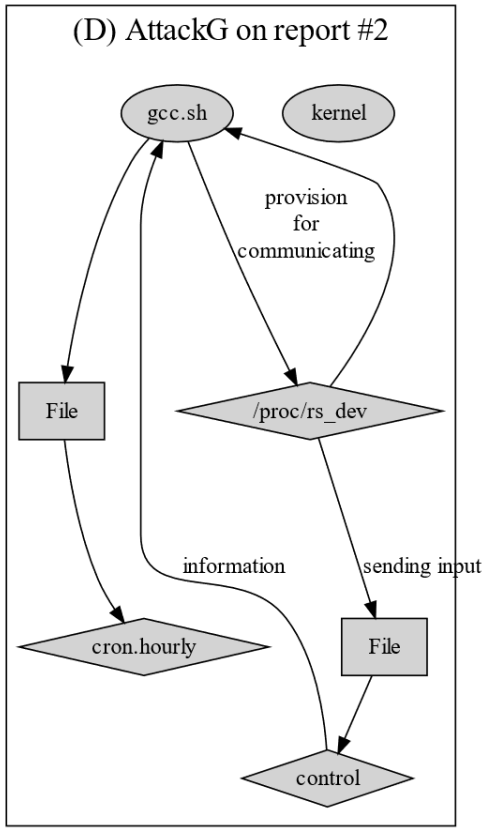

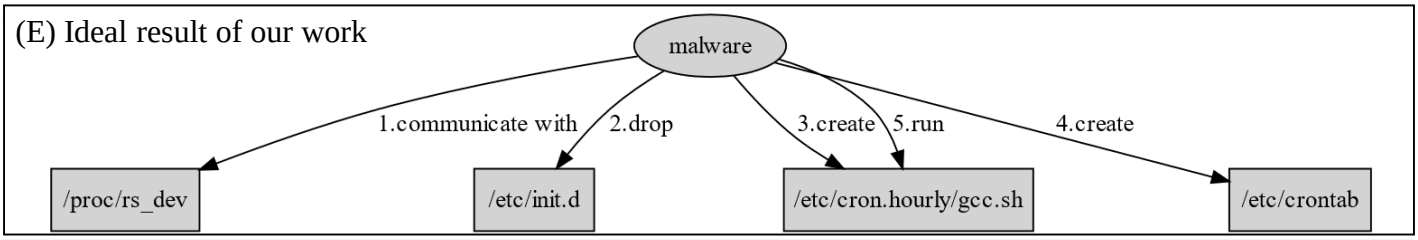

// Report 1 (source: intezer.com)

RedXOR uses an open-source LKM rootkit called “Adore-ng” to hide its process. Embedding open-source LKM rootkits is a common Winnti technique. The malware checks if the rootkit is active by creating a file and removing it. Then, the malware compares the “saved set-user-ID” of the process to the user ID. If they don’t match, the rootkit is enabled. As part of its persistence methods, RedXOR attempts to create a service under rc.d. The developer added “S99” before the name of the service to lower its priority and make it run last on system initiation.

// Report 2 (source: microsoft.com)

Some XorDdos samples install a kernel rootkit, while others embed the rootkit in the XorDdos binary. In this case, the malware has a provision for communicating with its rootkit component /proc/rs_dev by sending input and output control (IOCTL) calls with additional information to take appropriate action. XorDdos uses various persistence mechanisms to support different Linux distributions. The malware drops an init script at the location /etc/init.d. It creates a cron script at the location /etc/cron.hourly/gcc.sh then creates a /etc/crontab file to run /etc/cron.hourly/gcc.sh every three minutes.