Groundtruth

The Method of Labeling Groundtruth

We first identify the processes that are created by the identical parent processes and are related to each other by checking whether they have data dependency relationship (i.e. they are linked by resource nodes). Each group of the related processes are put into a community. We then label the parent process as the master process of the community, and associate the resource nodes (i.e. file node and network node) to the found communities according to their dependencies with the process nodes.

To further obtain more objective ground truths, we find three independent experts in computer system field to check the community ground truth. These experts all received Ph.D. degrees of computer science, and have deep understanding of computer system behaviors. The first expert engages in the Distributed System Management and System Log Analysis for more than 20 years. The second expert engages in System Log Analysis and Cloud Platform Management for more than 15 years, The third expert engages in High Performance Interconnects and Protocols and Big Data Computing for more than 10 years. We revised our ground truth according to their verification results. More specifically, if at least two experts considers a node should belong to a different community, then we will assign the nodes to the new community. For some nodes, the experts do not reach a consensus on the node assignment. For example, only one expert thinks the node should belong to the other community, or two experts consider the node should belong to two different communities. In these cases, we will not make any change of the node.

Groundtruth for attack dataset.

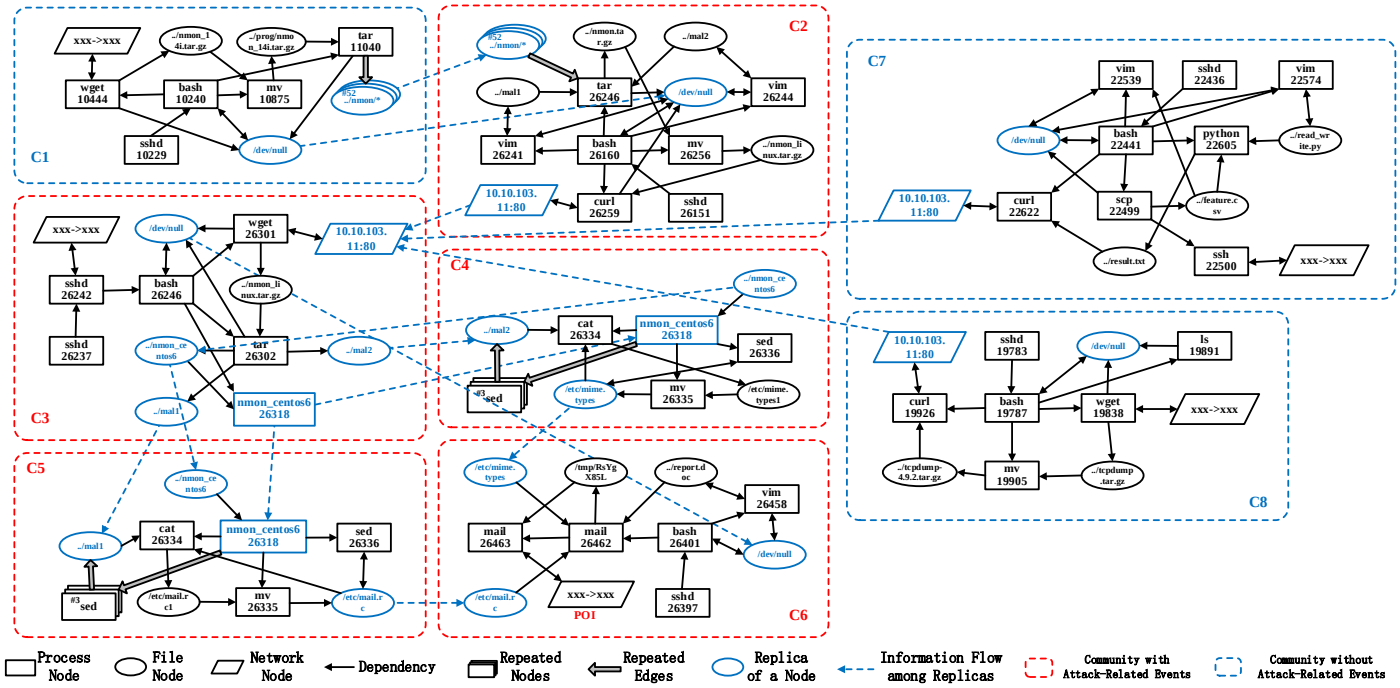

Figure 1: Groundtruth for Email Penetration (A1)

Figure 1 is our groundtruth for Email Penetration (A1). Expert 1 reaches a consensus on our node assignment. Expert 2 gives a revised suggestion: (1) file node ../nmon_centos6 is revised from C3,C4 and C5 to C3. Expert 3 gives two revised suggestion: (1) file node ../nmon_centos6 is revised from C3,C4 and C5 to C3, and (2) file node /etc/mail.rc is revised from C5 and C6 to C5. Since, the revised suggestion Expert 2 (1) and Expert 3 (1) reach a consensus, we make the revision according to the suggestion.

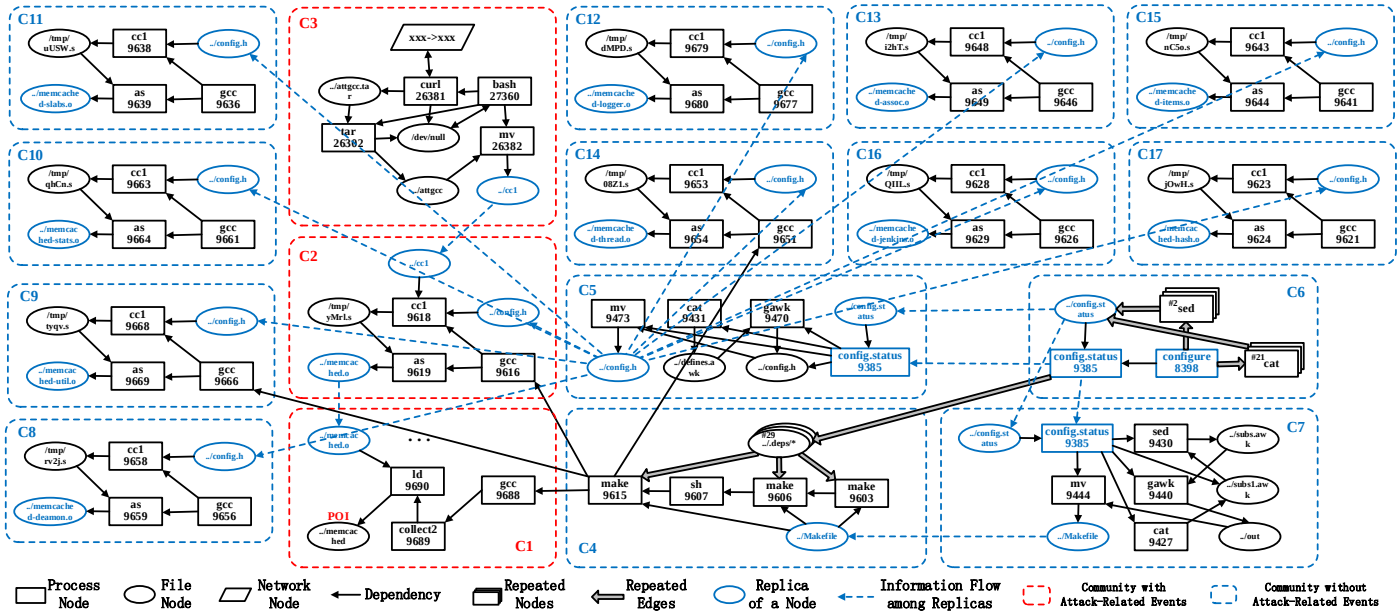

Figure 2: Groundtruth for Compile Crash (A2)

Figure 2 is our groundtruth for Compile Crash (A2). Expert 1 reaches a consensus on our node assignment. Expert 2 gives two revised suggestions: (1) file node ../config.status is revised from C5,C6 and C7 to C6, and (2) file node ../Makefile from C4 and C7 to C4. Expert 3 gives one revised suggestion: (1) file node . ../config.status is revised from C5,C6 and C7 to C6. Since, the revised suggestion Expert 2 (1) and Expert 3 (1) reach a consensus, we make the revision according to the suggestion.

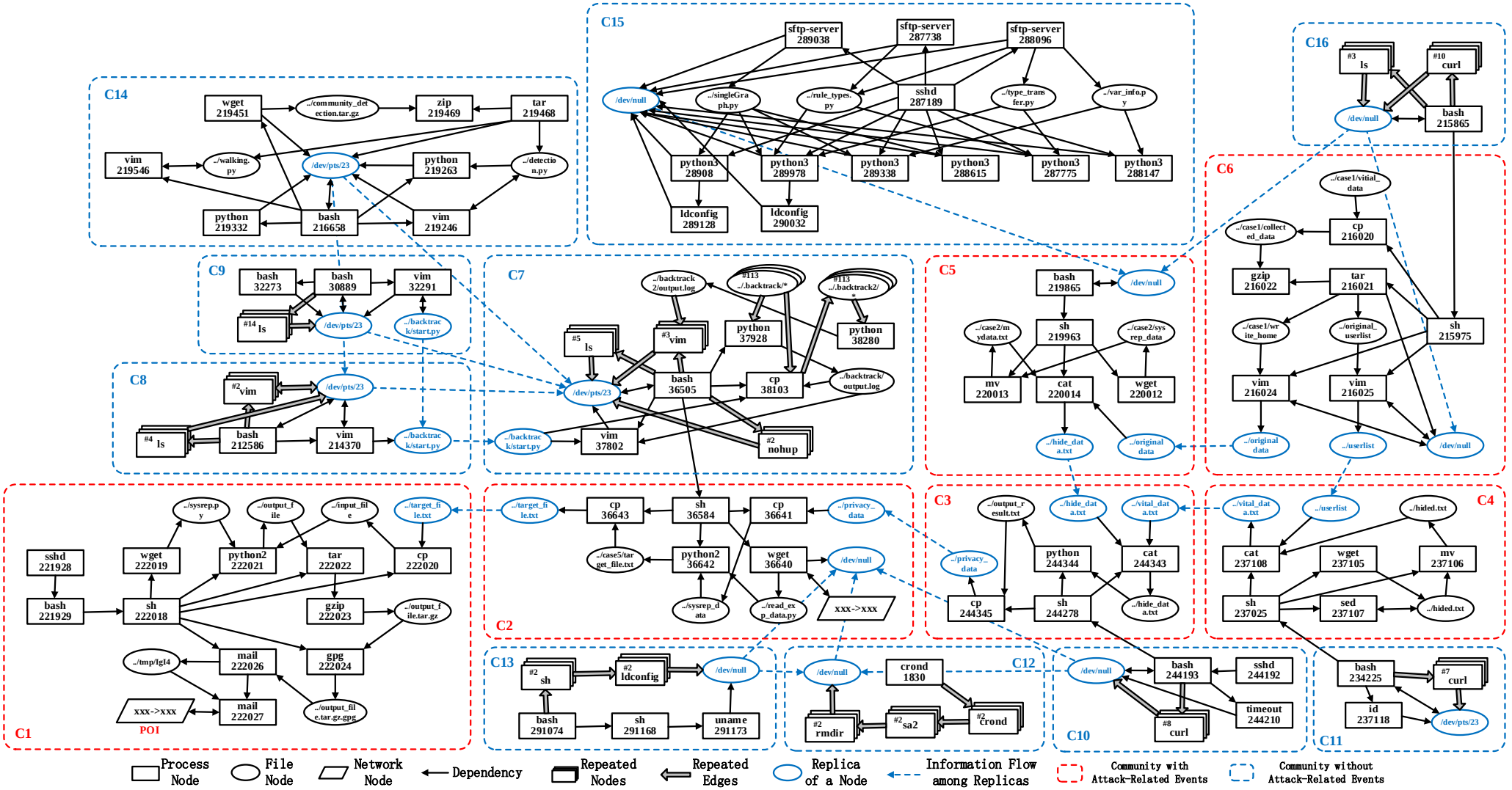

Figure 3: Groundtruth for Files Tamper (A3)

Figure 3 is our groundtruth for Files Tamper (A3). Expert 1 reaches a consensus on our node assignment. Expert 2 gives one revised suggestion: (1) file node ../backtrack/start.py is revised from C7,C8 and C9 to C7. Expert 3 reaches a consensus on our node assignment. Since, the revised suggestion Expert 2 (1) does not reach a consensus with the other experts, we do not make any revision.

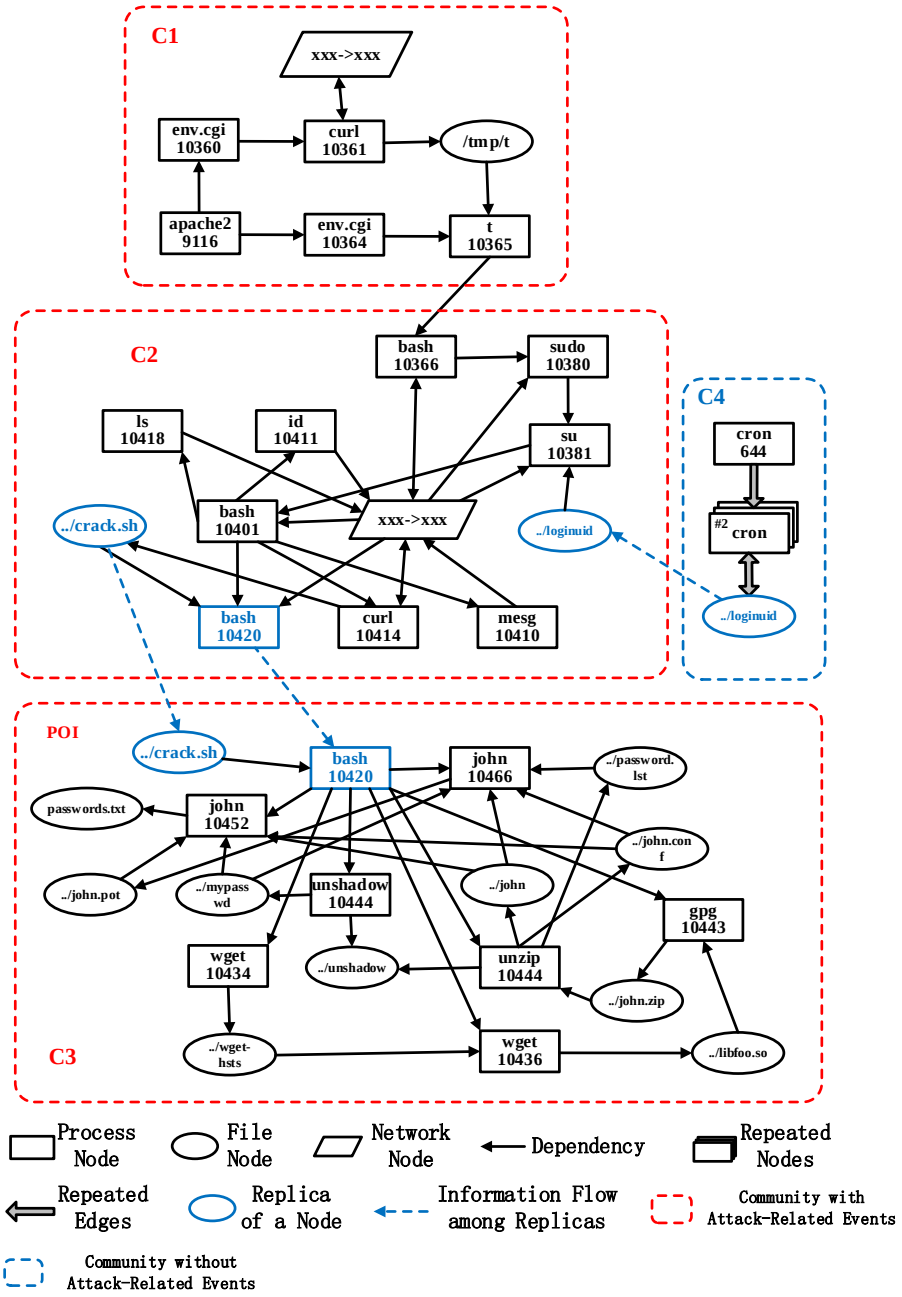

Figure 4: Groundtruth for Password Crack (A4)

Figure 4 is our groundtruth for Password Crack (A4). Expert 1 reaches a consensus on our node assignment. Expert 2 gives one revised suggestions: (1) file node ../crack.sh is revised from C2 and C3 to C2. Expert 3 gives one revised suggestion: (1) file node ../crack.sh is revised from C2 and C3 to C2. Since, the revised suggestion Expert 2 (1) and Expert 3 (1) reach a consensus, we make the revision according to the suggestion.

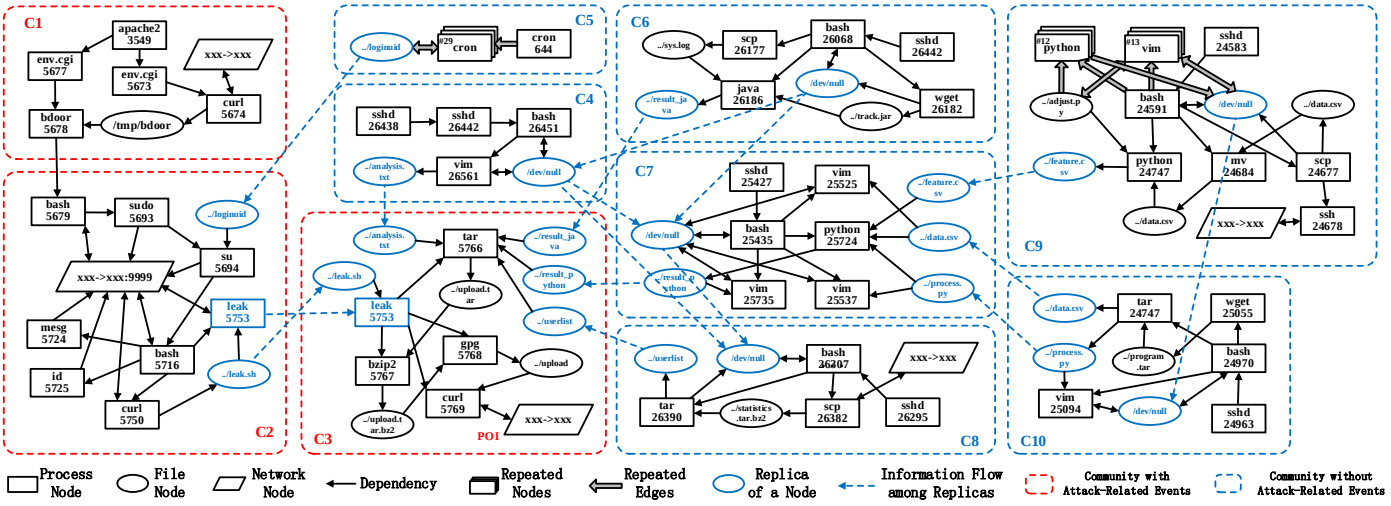

Figure 5: Groundtruth for Data Exfiltration (A5)

Figure 5 is our groundtruth for Data Exfiltration (A5). Expert 1 reaches a consensus on our node assignment. Expert 2 gives three revised suggestions: (1) file node ../leak.sh is revised from C2 and C3 to C2, (2) file node ../result_python from C3 and C7 to C7, and (3) file node ../data.csv from C7 and C10 to C7. Expert 3 gives one revised suggestion: (1) file node ../leak.sh is revised from C2 and C3 to C2. Since, the revised suggestion Expert 2 (1) and Expert 3 (1) reach a consensus, we make the revision according to the suggestion.

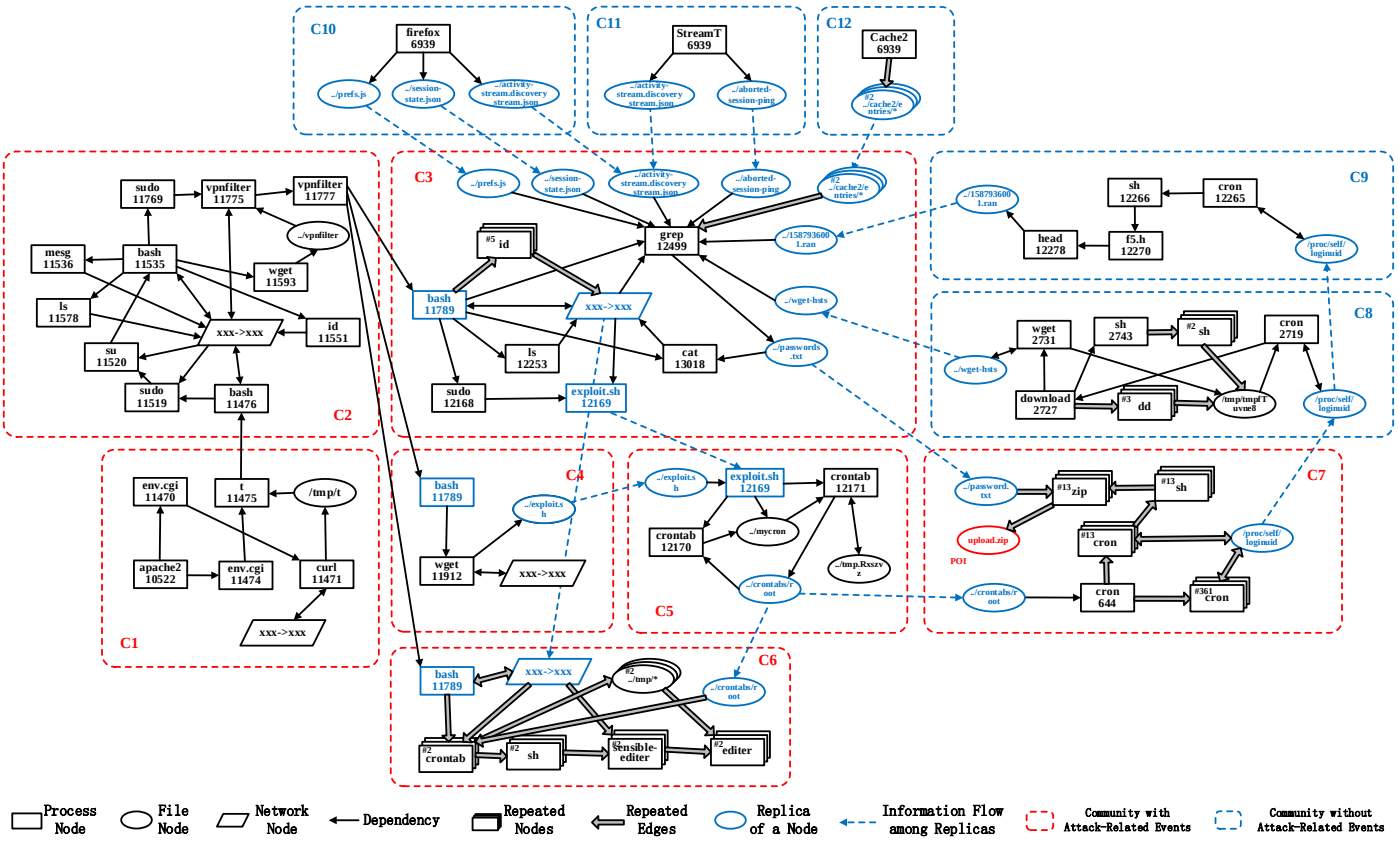

Figure 6: Groundtruth for VPN Filter (A6)

Figure 6 is our groundtruth for VPN Filter (A6). Expert 1 reaches a consensus on our node assignment. Expert 2 gives two revised suggestions: (1) file node ../exploit.sh is revised from C4 and C5 to C4, (2) file node ../crontabs/root from C5 and C7 to C5. Expert 3 gives one revised suggestion: (1) file node ../exploit.sh is revised from C4 and C5 to C4. Since, the revised suggestion Expert 2 (1) and Expert 3 (1) reach a consensus, we make the revision according to the suggestion.

Groundtruth for DARPA TC dataset

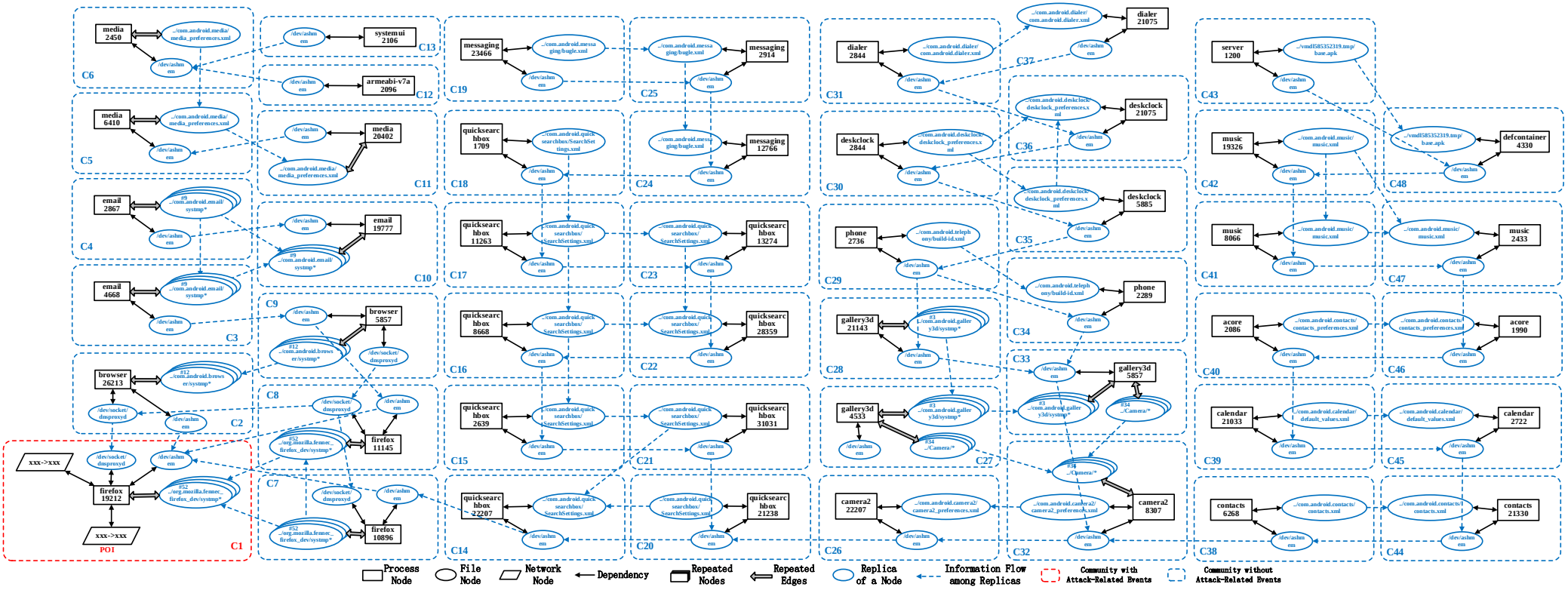

Figure 7: Groundtruth for Phishing Email (C.S.) (D1)

Figure 7 is our groundtruth for Phishing Email (C.S) (D1). Three experts all reach a consensus on our node assignment, so we does not make the revision.

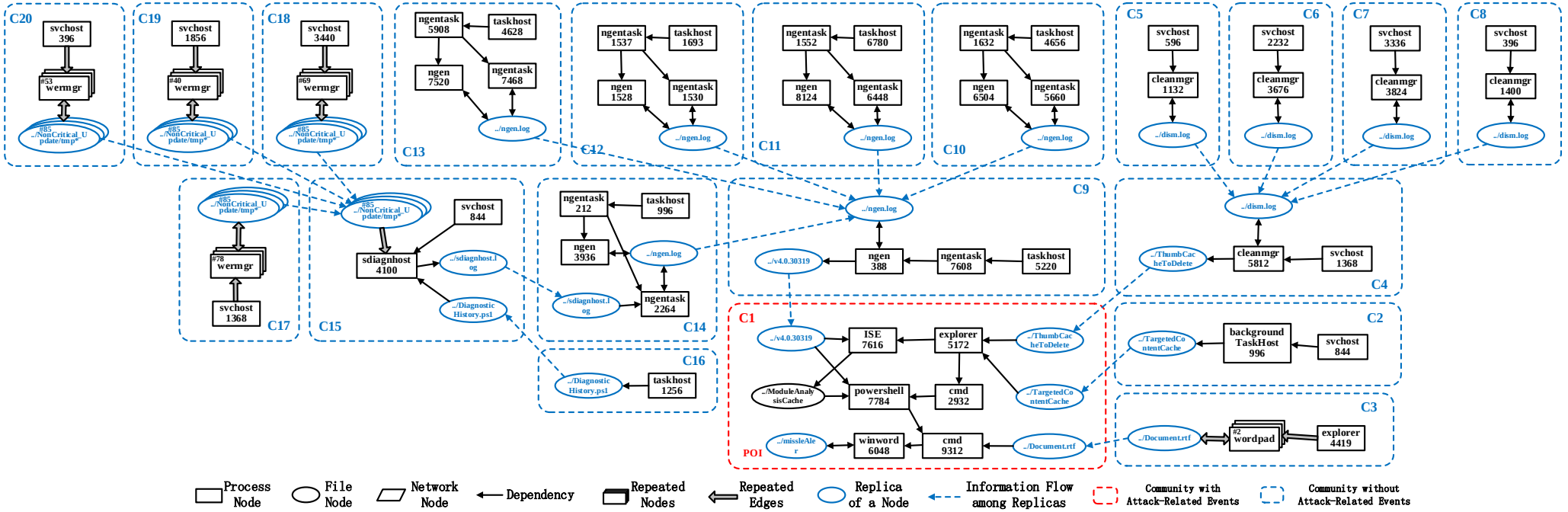

Figure 8: Groundtruth for Phishing Email (F.D.) (D2)

Figure 8 is our groundtruth for Phishing Email (F.D) (D2). Three experts all reach a consensus on our node assignment, so we does not make the revision.

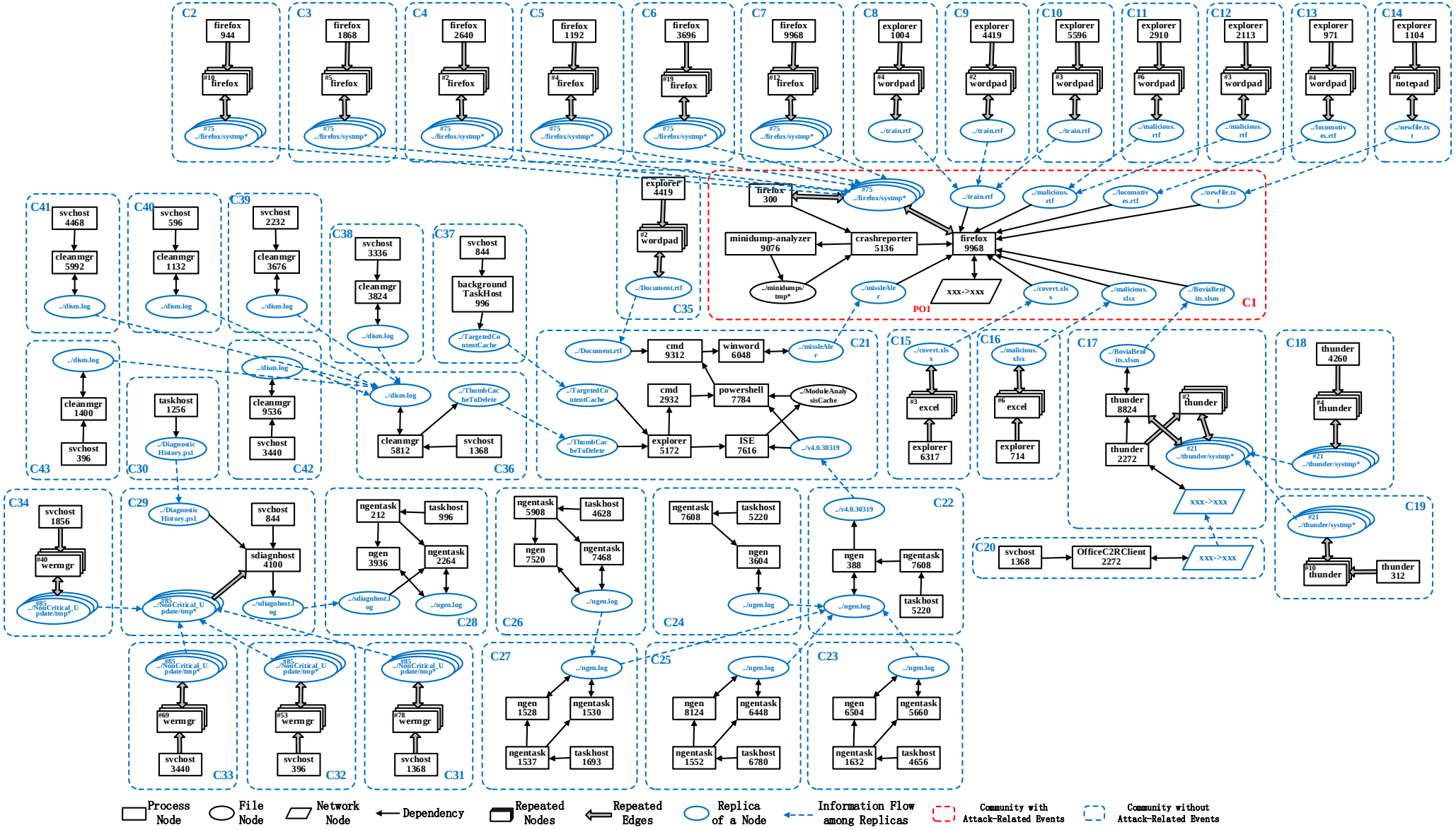

Figure 9: Groundtruth for Firefox Backdoor (F.D.) (D3)

Figure 9 is our groundtruth for Firefox Backdoor (F.D) (D3). Three experts all reach a consensus on our node assignment, so we does not make the revision.

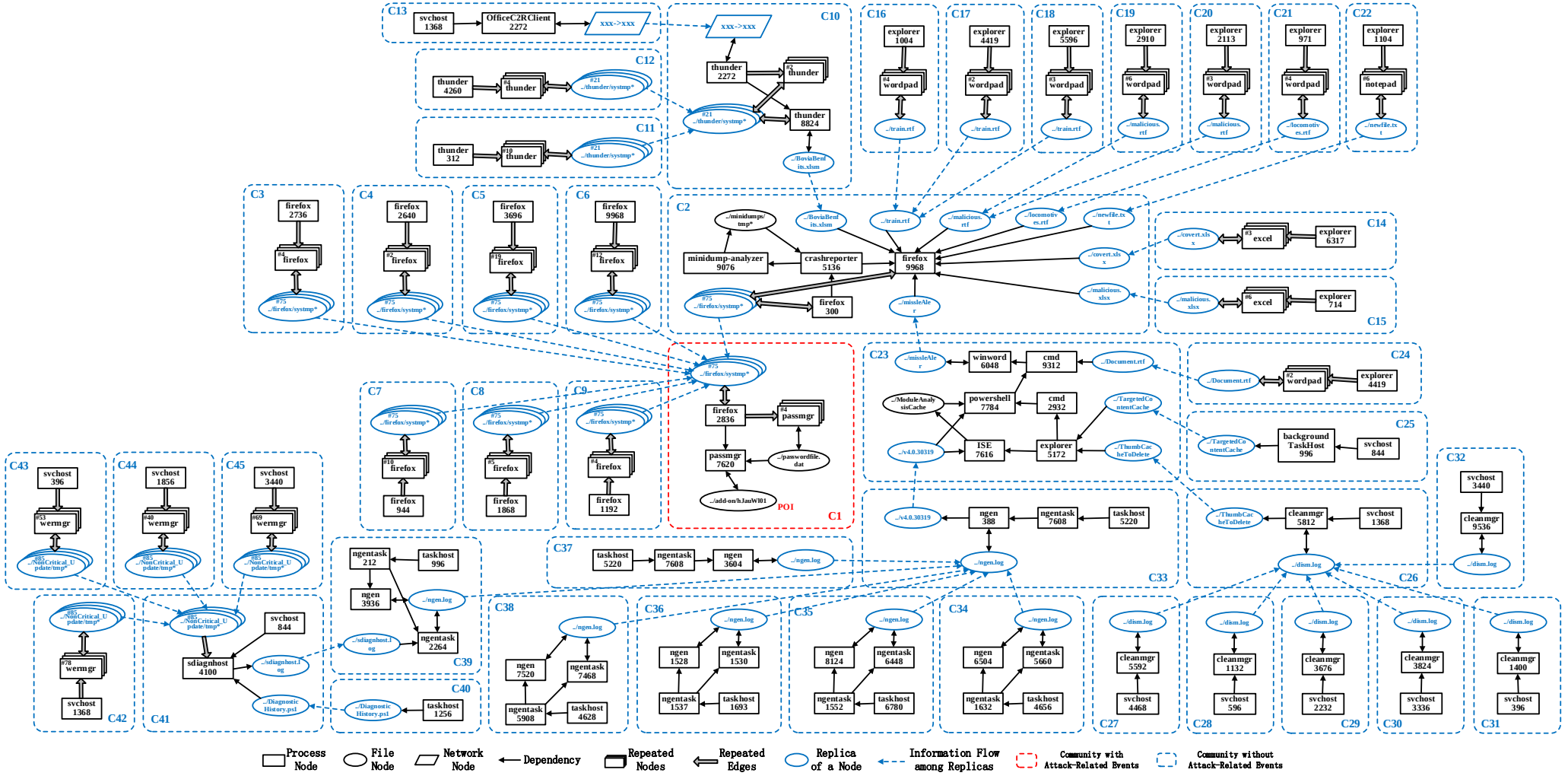

Figure 10: Groundtruth for Browser Extension (F.D.) (D4)

Figure 10 is our groundtruth for Browser Extension (F.D) (D4). Three experts all reach a consensus on our node assignment, so we does not make the revision.

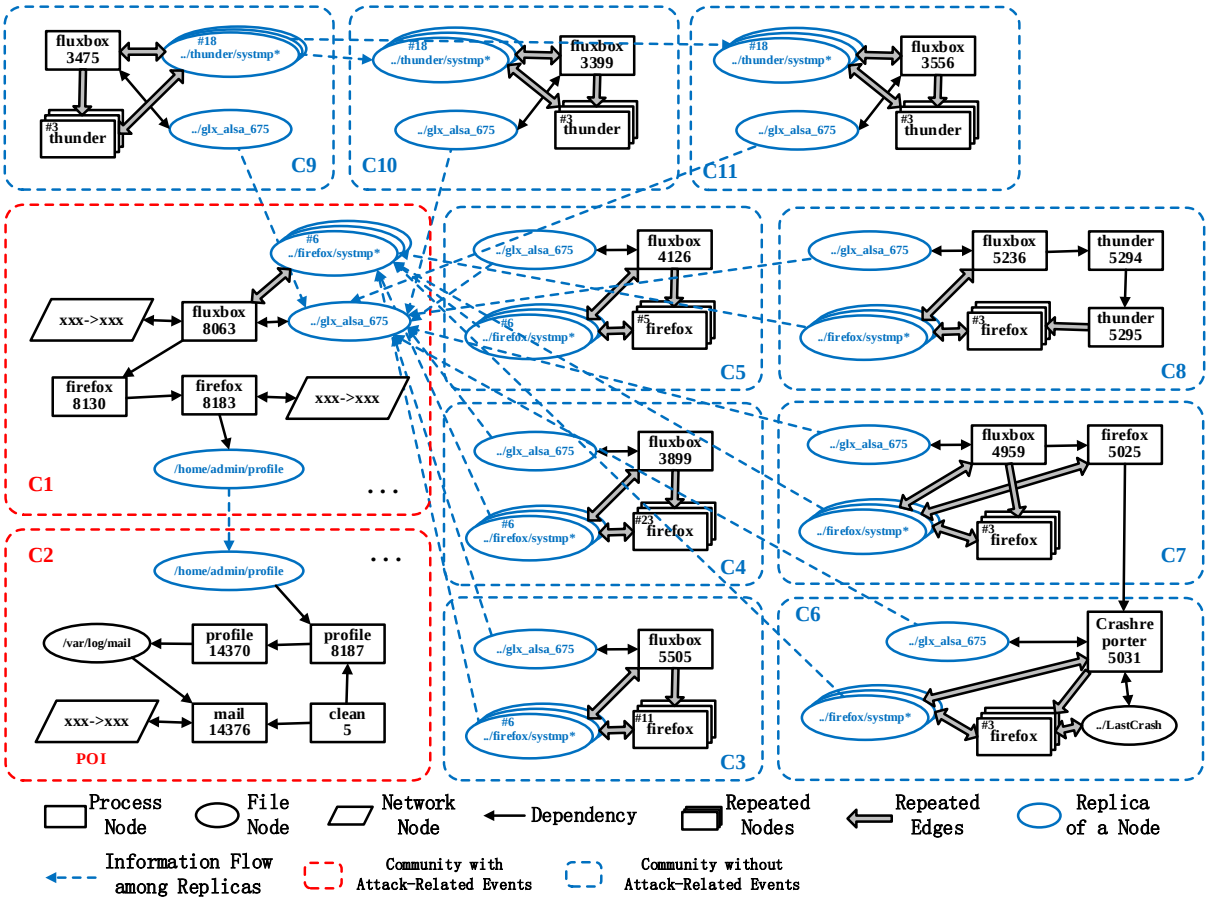

Figure 11: Groundtruth for Browser Extension (Theia) (D5)

Figure 11 is our groundtruth for Browser Extension (Theia) (D5). Three experts all reach a consensus on our node assignment, so we does not make the revision.

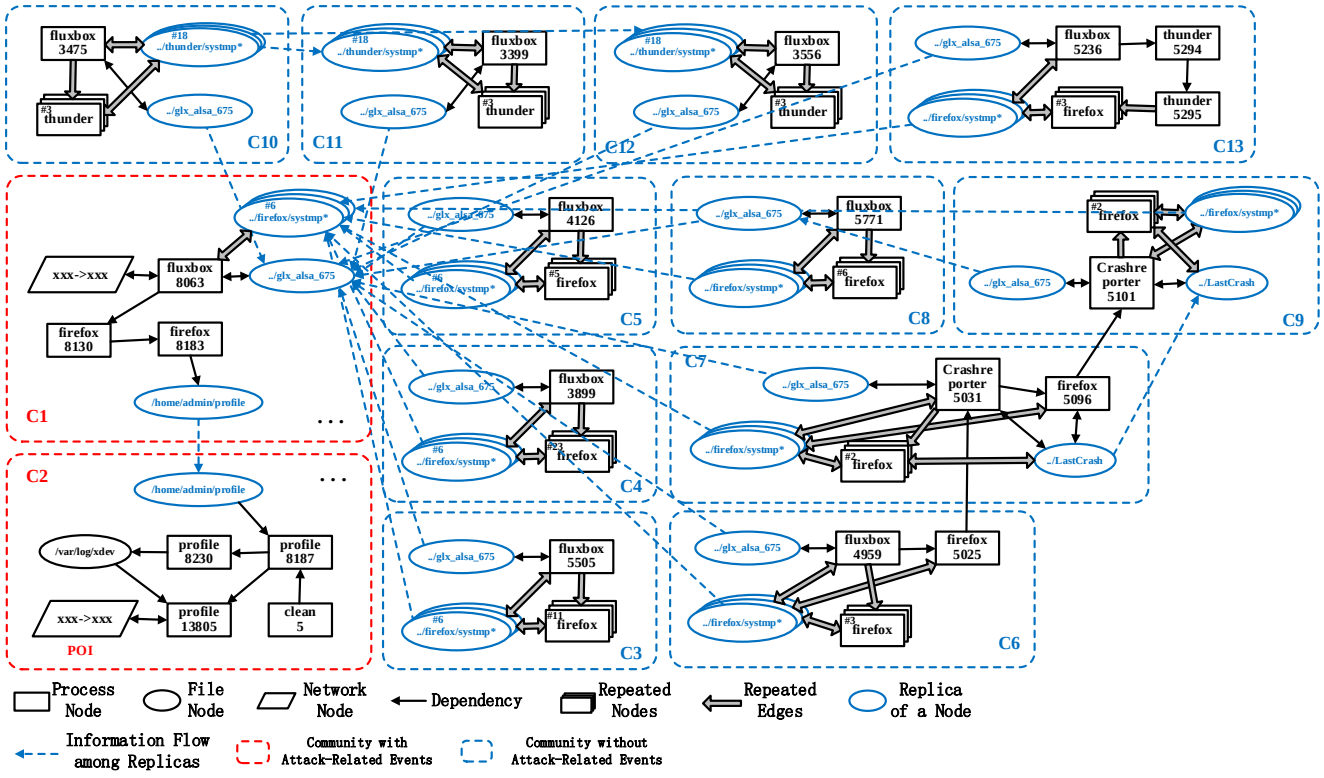

Figure 12: Groundtruth for Firefox Backdoor (Theia) (D6)

Figure 12 is our groundtruth for Firefox Backdoor (Theia) (D6). Three experts all reach a consensus on our node assignment, so we does not make the revision.

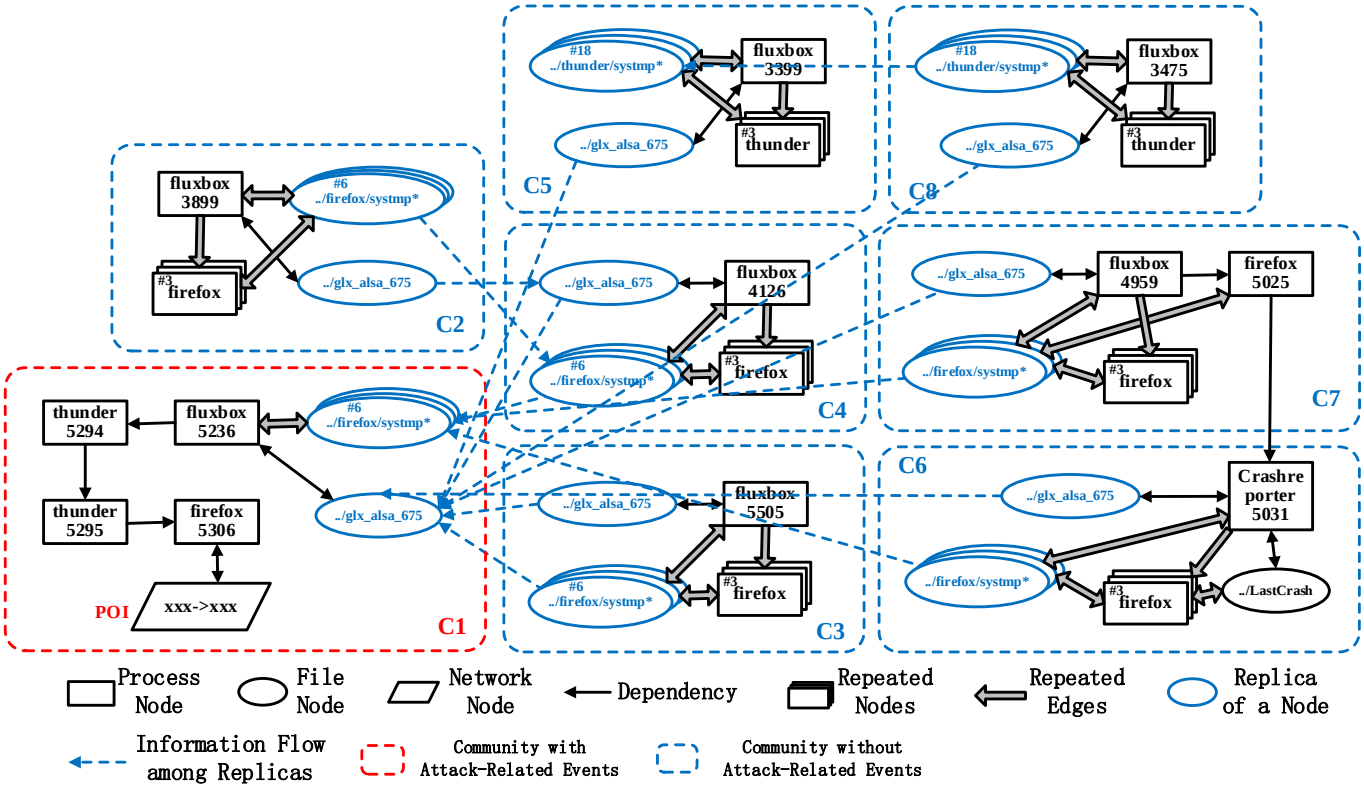

Figure 13: Groundtruth for Phishing Email (Theia) (D7)

Figure 13 is our groundtruth for Phishing Email (Theia) (D7). Three experts all reach a consensus on our node assignment, so we does not make the revision.

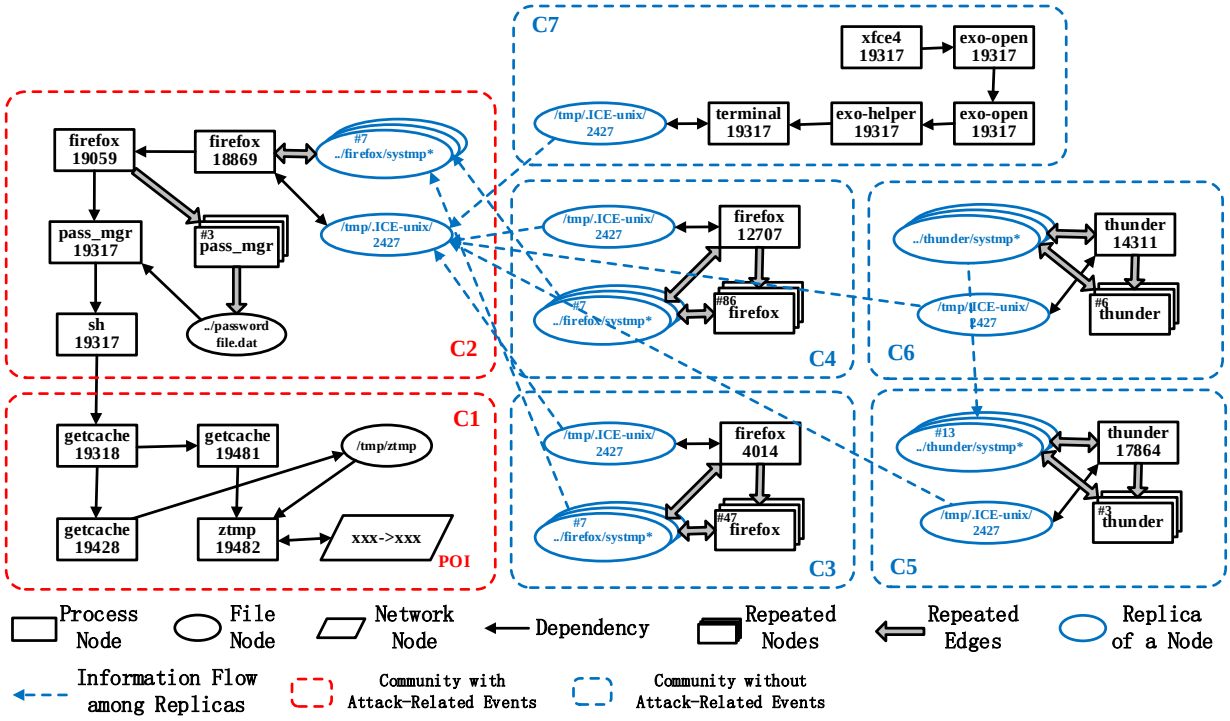

Figure 14: Groundtruth for Pine Backdoor (Trace) (D8)

Figure 14 is our groundtruth for Pine Backdoor (Trace) (D8). Three experts all reach a consensus on our node assignment, so we does not make the revision.