

JOeSandbox Cloud BASIC



ID: 397461

Sample Name: chVYyxhDuF

Cookbook:

defaultlinuxfilecookbook.jbs

Time: 20:10:15

Date: 25/04/2021

Version: 31.0.0 Emerald

Table of Contents

Table of Contents	2
Analysis Report chVYyxhDuF	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Yara Overview	4
Initial Sample	4
Signature Overview	4
AV Detection:	5
Spreading:	5
Data Obfuscation:	5
Mitre Att&ck Matrix	5
Behavior Graph	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Domains	6
URLs	6
Domains and IPs	6
Contacted Domains	6
URLs from Memory and Binaries	6
Contacted IPs	7
Public	7
General Information	7
Runtime Messages	7
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	9
General	9
Static ELF Info	9
ELF header	9
Program Segments	9
Network Behavior	9
Network Port Distribution	10
TCP Packets	10
UDP Packets	10
System Behavior	10
Analysis Process: chVYyxhDuF PID: 4579 Parent PID: 4519	10
General	10
File Activities	10
File Read	10
File Written	10
Analysis Process: chVYyxhDuF PID: 4590 Parent PID: 4579	10
General	10
File Activities	10
Directory Enumerated	10
Analysis Process: chVYyxhDuF PID: 4597 Parent PID: 4579	11
General	11
Analysis Process: chVYyxhDuF PID: 4598 Parent PID: 4597	11
General	11

Analysis Report chVYyxhDuF

Overview

General Information

Sample Name:	chVYyxhDuF
Analysis ID:	397461
MD5:	25fcab587d63652.
SHA1:	3c6ab806a10b40..
SHA256:	4f6c3f1b1c93e4f...
Infos:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:	56
Range:	0 - 100
Whitelisted:	false

Signatures

Multi AV Scanner detection for subm...

Opens /proc/net/* files useful for find...

Sample is packed with UPX

Detected TCP or UDP traffic on non...

Sample contains only a LOAD segm...

Yara signature match

Classification

Startup

- system is Inxubuntu1
 - chVYyxhDuF (PID: 4579, Parent: 4519, MD5: 25fcab587d636520065da8126b62db41) Arguments: /tmp/chVYyxhDuF
 - chVYyxhDuF New Fork (PID: 4590, Parent: 4579)
 - chVYyxhDuF New Fork (PID: 4597, Parent: 4579)
 - chVYyxhDuF New Fork (PID: 4598, Parent: 4597)
 - cleanup

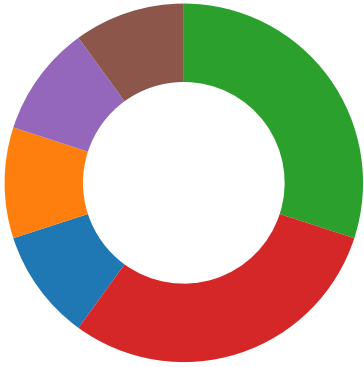
Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
chVYyxhDuF	SUSP_ELF_LNX_UPX_Compresed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	0x8708:\$s1: PROT_EXEC PROT_WRITE failed. 0x8777:\$s2: \$!d: UPX 0x8728:\$s3: \$!Info: This file is packed with the UPX executable packer

Signature Overview

- AV Detection
- Spreading
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior



Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Spreading:



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

Data Obfuscation:



Sample is packed with UPX

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	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Obfuscated Files or Information 1	OS Credential Dumping	Remote System Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Standard Port 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Behavior Graph



Contacted IPs



Public



IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.95.80.200	unknown	United States		36352	AS-COLOCROSSINGUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	397461
Start date:	25.04.2021
Start time:	20:10:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	chVYyxhDuF
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:	mal56.spre.evad.lin@0/1@0/0
Warnings:	Show All

Runtime Messages



Command:	/tmp/chVYyxhDuF
Exit Code:	0
Exit Code Info:	
Killed:	False

Standard Output:	Infected By Simps Botnet ;) Infected By Simps Botnet ;)
Standard Error:	

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	6WzIMKECB6	Get hash	malicious	Browse	23.95.80.200
	Ws1YobJVzp.dll	Get hash	malicious	Browse	107.172.227.10
	v3KWWCkmKW.dll	Get hash	malicious	Browse	107.172.227.10
	V9LdkRQa3y.dll	Get hash	malicious	Browse	107.172.227.10
	G0QfnXUA94.dll	Get hash	malicious	Browse	107.172.227.10
	WO4O1r4K1v.dll	Get hash	malicious	Browse	107.172.227.10
	1YfQ2n6lvf.dll	Get hash	malicious	Browse	107.172.227.10
	8GFukHv8PT.dll	Get hash	malicious	Browse	107.172.227.10
	M3dkfoVrTV.dll	Get hash	malicious	Browse	107.172.227.10
	WuqmlB8xq7.dll	Get hash	malicious	Browse	107.172.227.10
	iU85MrkJVV.dll	Get hash	malicious	Browse	107.172.227.10
	HbnmVuxDlc.exe	Get hash	malicious	Browse	23.94.150.194
	original title deed.xlsx	Get hash	malicious	Browse	172.245.45.28
	Purchase_Order_No_PO-4147074.xlsx	Get hash	malicious	Browse	198.23.207.82
	Purchase Order No. PO-4147074..xlsx	Get hash	malicious	Browse	198.23.207.82
	Autq1GcDD9.dll	Get hash	malicious	Browse	107.172.227.10
	guyYhasLYU.dll	Get hash	malicious	Browse	107.172.227.10
	22EiEfcKk1.dll	Get hash	malicious	Browse	107.172.227.10
	2OFJspIVtl.dll	Get hash	malicious	Browse	107.172.227.10
	Products List.xlsx	Get hash	malicious	Browse	198.23.213.57

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/tmp/keksec.infected.you.log	
Process:	/tmp/chVYyxhDuF
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	59
Entropy (8bit):	4.250767202963639
Encrypted:	false
SSDEEP:	3:7QTAfDM37Q+4Kyn:hDYU+4Kyn
MD5:	4BAAA04679A9403A2A594925DED1453B
SHA1:	8CDBC5F05BAB106C579075C26A1E5561EA37BA9B

/tmp/keksec.infected.you.log	
SHA-256:	0D3D80141438D9CD7F5501E3AB73DE9DE028F591BB198BC0290962E6F6F09C8D
SHA-512:	42820CFF50B3BD4C978152D3F4C86903C4750F054D358A77B242EEBAD7F574D35FED3FA7A16A1F8524315F87F3716EC540807E42A15AFD024D6D30749F48F816
Malicious:	false
Reputation:	low
Preview:	youve been infected by urmommy, thanks for joining keksec..

Static File Info

General	
File type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.979343394737344
TrID:	ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	chVYyxhDuF
File size:	52932
MD5:	25fcab587d636520065da8126b62db41
SHA1:	3c6ab806a10b40af8dd70825fc0aa8ae68b9dab4
SHA256:	4f6c3f1b1c93e4f5363fe2c472ad6a7d76f825f3b252df8cb4172e45474b6648
SHA512:	4b13bb48de87b0e357b8c36b069f5bb2a359eba1d9cda569490d97bf1cfa8b11efb91cdc4f7e211a3c8b6c072a880f1ade2897209af38deeca28916b9664ffa3
SSDEEP:	1536:XjTLuOqoZuuVpbpcef7p7PgZEcgOoDFbGVyHYH9f:zTLuOqtuVNJNTgKfOk3HYf
File Content Preview:	.ELF.....>.....p@.....@.8...@.....P.....P.Q....P.Q.....Q.td.....;G.cU PXID.....

Static ELF Info

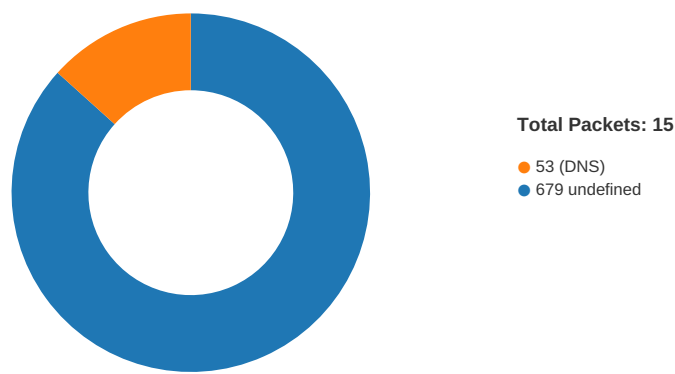
ELF header	
Class:	ELF64
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Advanced Micro Devices X86-64
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x107c70
Flags:	0x0
ELF Header Size:	64
Program Header Offset:	64
Program Header Size:	56
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	64
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x100000	0x100000	0x8dac	0x8dac	0x5	R E	0x100000		
LOAD	0xe50	0x518e50	0x518e50	0x0	0x0	0x6	RW	0x1000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0x6	RW	0x8		

Network Behavior

Network Port Distribution



TCP Packets

UDP Packets

System Behavior

Analysis Process: chVYyxhDuF PID: 4579 Parent PID: 4519

General

Start time:	20:10:45
Start date:	25/04/2021
Path:	/tmp/chVYyxhDuF
Arguments:	/tmp/chVYyxhDuF
File size:	52932 bytes
MD5 hash:	25fcab587d636520065da8126b62db41

File Activities

File Read

File Written

Analysis Process: chVYyxhDuF PID: 4590 Parent PID: 4579

General

Start time:	20:10:45
Start date:	25/04/2021
Path:	/tmp/chVYyxhDuF
Arguments:	n/a
File size:	52932 bytes
MD5 hash:	25fcab587d636520065da8126b62db41

File Activities

Directory Enumerated

Analysis Process: chVYyxhDuF PID: 4597 Parent PID: 4579



General



Start time:	20:10:45
Start date:	25/04/2021
Path:	/tmp/chVYyxhDuF
Arguments:	n/a
File size:	52932 bytes
MD5 hash:	25fcab587d636520065da8126b62db41

Analysis Process: chVYyxhDuF PID: 4598 Parent PID: 4597



General



Start time:	20:10:45
Start date:	25/04/2021
Path:	/tmp/chVYyxhDuF
Arguments:	n/a
File size:	52932 bytes
MD5 hash:	25fcab587d636520065da8126b62db41