

JOeSandbox Cloud BASIC



ID: 756104

Sample Name:

DiskMaker_X_9.dmg

Cookbook:

defaultmacfilecookbook.jbs

Time: 16:37:54

Date: 29/11/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
macOS Analysis Report DiskMaker_X_9.dmg	6
Overview	6
General Information	6
Detection	6
Signatures	6
Classification	6
General Information	6
Warnings	6
Runtime Messages	6
Process Tree	6
Yara Signatures	7
Snort Signatures	8
Joe Sandbox Signatures	8
Mitre Att&ck Matrix	8
Behavior Graph	8
Screenshots	9
Thumbnails	9
Antivirus, Machine Learning and Genetic Malware Detection	10
Initial Sample	10
Dropped Files	10
Domains	10
URLs	10
Domains and IPs	10
Contacted Domains	10
Contacted URLs	11
World Map of Contacted IPs	11
Public IPs	11
Joe Sandbox View / Context	11
IPs	11
Domains	11
ASNs	11
JA3 Fingerprints	11
Dropped Files	12
Created / dropped Files	12
/Users/berri/Library/Logs/DiskMakerX.log	12
/dev/null	12
Static File Info	12
General	12
CodeSign Information	12
Network Behavior	12
Network Port Distribution	12
TCP Packets	12
UDP Packets	12
ICMP Packets	12
DNS Queries	13
DNS Answers	13
HTTP Request Dependency Graph	13
System Behavior	13
Analysis Process: mono-sgen32 PID: 892, Parent PID: 812	13
General	13
Analysis Process: open PID: 892, Parent PID: 812	13
General	13
File Activities	13
File Read	13
Directory Enumerated	13
Analysis Process: xpcproxy PID: 893, Parent PID: 1	13
General	13
File Activities	13
File Read	13
Directory Created	13
Analysis Process: applet PID: 893, Parent PID: 1	14
General	14
File Activities	14
File Read	14
File Written	14
Directory Enumerated	14
Directory Attributes Enumerated Bulk	14
Directory Created	14
Analysis Process: applet PID: 894, Parent PID: 893	14
General	14
Analysis Process: sh PID: 894, Parent PID: 893	14
General	14
File Activities	14
File Read	14
Analysis Process: applet PID: 895, Parent PID: 893	14
General	14

Analysis Process: sh PID: 895, Parent PID: 893	14
General	14
File Activities	14
File Read	15
Analysis Process: touch PID: 895, Parent PID: 893	15
General	15
File Activities	15
File Created	15
File Read	15
Analysis Process: applet PID: 896, Parent PID: 893	15
General	15
Analysis Process: sh PID: 896, Parent PID: 893	15
General	15
File Activities	15
File Read	15
File Written	15
Analysis Process: applet PID: 897, Parent PID: 893	15
General	15
Analysis Process: sh PID: 897, Parent PID: 893	15
General	15
File Activities	15
File Read	16
Analysis Process: sh PID: 898, Parent PID: 897	16
General	16
Analysis Process: date PID: 898, Parent PID: 897	16
General	16
File Activities	16
File Read	16
File Written	16
Analysis Process: applet PID: 899, Parent PID: 893	16
General	16
Analysis Process: sh PID: 899, Parent PID: 893	16
General	16
File Activities	16
File Read	16
File Written	16
Analysis Process: applet PID: 900, Parent PID: 893	16
General	16
Analysis Process: sh PID: 900, Parent PID: 893	16
General	17
File Activities	17
File Read	17
Analysis Process: defaults PID: 900, Parent PID: 893	17
General	17
File Activities	17
File Read	17
Directory Enumerated	17
Analysis Process: applet PID: 901, Parent PID: 893	17
General	17
Analysis Process: sh PID: 901, Parent PID: 893	17
General	17
File Activities	17
File Read	17
File Written	17
Analysis Process: applet PID: 902, Parent PID: 893	17
General	17
Analysis Process: sh PID: 902, Parent PID: 893	17
General	18
File Activities	18
File Read	18
Analysis Process: sh PID: 903, Parent PID: 902	18
General	18
Analysis Process: sw_vers PID: 903, Parent PID: 902	18
General	18
File Activities	18
File Read	18
Directory Enumerated	18
Analysis Process: sh PID: 904, Parent PID: 902	18
General	18
Analysis Process: cut PID: 904, Parent PID: 902	18
General	18
File Activities	18
File Read	18
Analysis Process: applet PID: 905, Parent PID: 893	18
General	18
Analysis Process: sh PID: 905, Parent PID: 893	19
General	19
File Activities	19
File Read	19
Analysis Process: sh PID: 906, Parent PID: 905	19
General	19
Analysis Process: sw_vers PID: 906, Parent PID: 905	19
General	19
File Activities	19
File Read	19
Directory Enumerated	19
Analysis Process: sh PID: 907, Parent PID: 905	19
General	19
Analysis Process: cut PID: 907, Parent PID: 905	19
General	19
File Activities	20
File Read	20
Analysis Process: applet PID: 908, Parent PID: 893	20
General	20
Analysis Process: sh PID: 908, Parent PID: 893	20

General	20
File Activities	20
File Read	20
Analysis Process: sh PID: 909, Parent PID: 908	20
General	20
Analysis Process: sw_vers PID: 909, Parent PID: 908	20
General	20
File Activities	20
File Read	20
Directory Enumerated	20
Analysis Process: sh PID: 910, Parent PID: 908	20
General	20
Analysis Process: cut PID: 910, Parent PID: 908	21
General	21
File Activities	21
File Read	21
Analysis Process: applet PID: 911, Parent PID: 893	21
General	21
Analysis Process: sh PID: 911, Parent PID: 893	21
General	21
File Activities	21
File Read	21
Analysis Process: sh PID: 912, Parent PID: 911	21
General	21
Analysis Process: sw_vers PID: 912, Parent PID: 911	21
General	21
File Activities	21
File Read	21
Directory Enumerated	21
Analysis Process: sh PID: 913, Parent PID: 911	22
General	22
Analysis Process: cut PID: 913, Parent PID: 911	22
General	22
File Activities	22
File Read	22
Analysis Process: applet PID: 914, Parent PID: 893	22
General	22
Analysis Process: sh PID: 914, Parent PID: 893	22
General	22
File Activities	22
File Read	22
File Written	22
Analysis Process: applet PID: 915, Parent PID: 893	22
General	22
Analysis Process: sh PID: 915, Parent PID: 893	22
General	22
File Activities	23
File Read	23
Analysis Process: id PID: 915, Parent PID: 893	23
General	23
File Activities	23
File Read	23
Analysis Process: applet PID: 916, Parent PID: 893	23
General	23
Analysis Process: sh PID: 916, Parent PID: 893	23
General	23
File Activities	23
File Read	23
File Written	23
Analysis Process: applet PID: 917, Parent PID: 893	23
General	23
Analysis Process: sh PID: 917, Parent PID: 893	23
General	23
File Activities	24
File Read	24
Analysis Process: ps PID: 917, Parent PID: 893	24
General	24
File Activities	24
File Read	24
Directory Enumerated	24
Analysis Process: applet PID: 918, Parent PID: 893	24
General	24
Analysis Process: sh PID: 918, Parent PID: 893	24
General	24
File Activities	24
File Read	24
File Written	24
Analysis Process: applet PID: 919, Parent PID: 893	24
General	24
Analysis Process: sh PID: 919, Parent PID: 893	24
General	24
File Activities	25
File Read	25
Analysis Process: curl PID: 919, Parent PID: 893	25
General	25
File Activities	25
File Read	25
Analysis Process: applet PID: 920, Parent PID: 893	25
General	25
Analysis Process: sh PID: 920, Parent PID: 893	25
General	25
File Activities	25
File Read	25
File Written	25
Analysis Process: applet PID: 921, Parent PID: 893	25

General	25
Analysis Process: sh PID: 921, Parent PID: 893	25
General	25
File Activities	26
File Read	26
Analysis Process: sh PID: 922, Parent PID: 921	26
General	26
Analysis Process: mdfind PID: 922, Parent PID: 921	26
General	26
File Activities	26
File Read	26
Directory Enumerated	26
Analysis Process: sh PID: 923, Parent PID: 921	26
General	26
Analysis Process: grep PID: 923, Parent PID: 921	26
General	26
File Activities	26
File Read	26
Analysis Process: sh PID: 924, Parent PID: 921	26
General	26
Analysis Process: head PID: 924, Parent PID: 921	27
General	27
File Activities	27
File Read	27
Analysis Process: applet PID: 925, Parent PID: 893	27
General	27
Analysis Process: sh PID: 925, Parent PID: 893	27
General	27
File Activities	27
File Read	27
Analysis Process: sh PID: 926, Parent PID: 925	27
General	27
Analysis Process: sh PID: 927, Parent PID: 925	27
General	27
Analysis Process: wc PID: 927, Parent PID: 925	27
General	27
File Activities	28
File Read	28
Analysis Process: automountd PID: 928, Parent PID: 837	28
General	28
Analysis Process: od_user_homes PID: 928, Parent PID: 837	28
General	28
File Activities	28
File Read	28

macOS Analysis Report

DiskMaker_X_9.dmg

Overview

General Information

Sample Name:	DiskMaker_X_9.dmg
Analysis ID:	756104
MD5:	d575c6a4027834..
SHA1:	87d92610155135..
SHA256:	96845cd3755434..
Infos:	

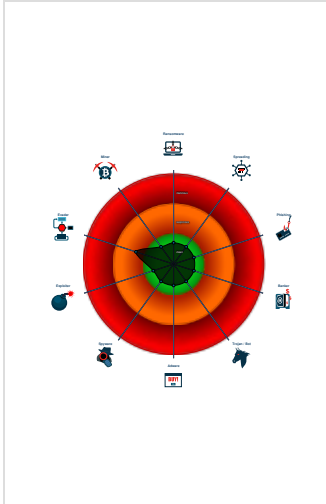
Detection

MALICIOUS SUSPICIOUS CLEAN UNKNOWN	
Score:	8
Range:	0 - 100
Whitelisted:	false

Signatures

Uses AppleScript framework/compo...
Reads the systems hostname
Reads the kernel OS version value
Executes the "grep" command used...
Reads the sysctl safe boot value (p...
Executes the "ps" command used t...
Queries OS software version with sh...
Executes the "curl" command used ...
Reads launchservices plist files
Uses AppleScript scripting additions...
Reads hardware related sysctl values

Classification



General Information	
Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756104
Start date and time:	2022-11-29 16:37:54 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DiskMaker_X_9.dmg
Cookbook file name:	defaultmacfilecookbook.jbs
Analysis system description:	Virtual Machine, High Sierra (Office 2016 16.16, Java 11.0.2+9, Adobe Reader 2019.010.20099)
Analysis Mode:	default
Detection:	CLEAN
Classification:	clean8.macDMG@0/9@1/0

Warnings	
Runtime Messages	
Command:	open "/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app"
PID:	892
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	

Process Tree

- **System is macvm-highsierra**
- **mono-sgen32** New Fork (PID: 892, Parent: 812)
- **open** (MD5: 40ed6d8f35c9f20484b97582d296398f) Arguments:
- **xpcproxy** New Fork (PID: 893, Parent: 1)
- **applet** (MD5: 0717bb720584b8dc860a0b9e235dd447) Arguments: /Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet
 - **applet** New Fork (PID: 894, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c echo \$HOME
 - **applet** New Fork (PID: 895, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c touch '/Users/berri/Library/Logs/DiskMakerX.log
 - **touch** (MD5: 4aacabad02929f18b00a9b6ef85e0605) Arguments: touch /Users/berri/Library/Logs/DiskMakerX.log
 - **applet** New Fork (PID: 896, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c echo '-----' >> '/Users/berri/Library/Logs/DiskMakerX.log
 - **applet** New Fork (PID: 897, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c date >> '/Users/berri/Library/Logs/DiskMakerX.log
 - **sh** New Fork (PID: 898, Parent: 897)
 - **date** (MD5: e1d20c480fcdc1ac4646170b1d9ca7c7) Arguments: date
 - **applet** New Fork (PID: 899, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c echo 'Home Path: ' '/Users/berri>> '/Users/berri/Library/Logs/DiskMakerX.log
 - **applet** New Fork (PID: 900, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c defaults read NSGlobalDomain AppleLanguages
 - **defaults** (MD5: 831678c94c2d9c647bf3d283b1861bda) Arguments: defaults read NSGlobalDomain AppleLanguages
 - **applet** New Fork (PID: 901, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c echo 'Current Language: ' 'en-CH>> '/Users/berri/Library/Logs/DiskMakerX.log
 - **applet** New Fork (PID: 902, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c sw_vers -productVersion | cut -c 1-4
 - **sh** New Fork (PID: 903, Parent: 902)
 - **sw_vers** (MD5: d33f7f9efd4158694d0d58879b54f89d) Arguments: sw_vers -productVersion
 - **sh** New Fork (PID: 904, Parent: 902)
 - **cut** (MD5: e27c92637d672468ea846d377b500eb1) Arguments: cut -c 1-4
 - **applet** New Fork (PID: 905, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c sw_vers -productVersion | cut -c 4-4
 - **sh** New Fork (PID: 906, Parent: 905)
 - **sw_vers** (MD5: d33f7f9efd4158694d0d58879b54f89d) Arguments: sw_vers -productVersion
 - **sh** New Fork (PID: 907, Parent: 905)
 - **cut** (MD5: e27c92637d672468ea846d377b500eb1) Arguments: cut -c 4-4
 - **applet** New Fork (PID: 908, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c sw_vers -productVersion | cut -c 1-5
 - **sh** New Fork (PID: 909, Parent: 908)
 - **sw_vers** (MD5: d33f7f9efd4158694d0d58879b54f89d) Arguments: sw_vers -productVersion
 - **sh** New Fork (PID: 910, Parent: 908)
 - **cut** (MD5: e27c92637d672468ea846d377b500eb1) Arguments: cut -c 1-5
 - **applet** New Fork (PID: 911, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c sw_vers -productVersion | cut -c 4-5
 - **sh** New Fork (PID: 912, Parent: 911)
 - **sw_vers** (MD5: d33f7f9efd4158694d0d58879b54f89d) Arguments: sw_vers -productVersion
 - **sh** New Fork (PID: 913, Parent: 911)
 - **cut** (MD5: e27c92637d672468ea846d377b500eb1) Arguments: cut -c 4-5
 - **applet** New Fork (PID: 914, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c echo 'Current OS: ' '10.13>> '/Users/berri/Library/Logs/DiskMakerX.log
 - **applet** New Fork (PID: 915, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c id -G
 - **id** (MD5: 24c45eb23e1aae68c572939d1a906018) Arguments: id -G
 - **applet** New Fork (PID: 916, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c echo 'Is this user an admin : ' 'true>> '/Users/berri/Library/Logs/DiskMakerX.log
 - **applet** New Fork (PID: 917, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c ps auxc
 - **ps** (MD5: 792e18b1417ac1f184680d2423206e4f) Arguments: ps auxc
 - **applet** New Fork (PID: 918, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c echo 'Path Finder launched : ' 'false>> '/Users/berri/Library/Logs/DiskMakerX.log
 - **applet** New Fork (PID: 919, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c curl http://diskmakerx.com/CurrentLDMVersion
 - **curl** (MD5: 078cd73f58d3d8f875eed22522ff73f7) Arguments: curl http://diskmakerx.com/CurrentLDMVersion
 - **applet** New Fork (PID: 920, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c echo 'Selected OS: ' '10.15>> '/Users/berri/Library/Logs/DiskMakerX.log
 - **applet** New Fork (PID: 921, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c mdfind -name 'Install macOS Catalina' | grep -v Library | head -1
 - **sh** New Fork (PID: 922, Parent: 921)
 - **mdfind** (MD5: 84f3a3da590e65271df7fecb27671fac) Arguments: mdfind -name Install macOS Catalina
 - **sh** New Fork (PID: 923, Parent: 921)
 - **grep** (MD5: 2b3efb273296881708ea2914c612e0eb) Arguments: grep -v Library
 - **sh** New Fork (PID: 924, Parent: 921)
 - **head** (MD5: bb2984cc21ccc7343bed41f2b577c011) Arguments: head -1
 - **applet** New Fork (PID: 925, Parent: 893)
 - **sh** (MD5: 8aa60b22a5d30418a002b340989384dc) Arguments: sh -c echo " | wc -l
 - **sh** New Fork (PID: 926, Parent: 925)
 - **sh** New Fork (PID: 927, Parent: 925)
 - **wc** (MD5: b89949ce6a1929257e5c0c157027cbfe) Arguments: wc -l
 - **automountd** New Fork (PID: 928, Parent: 837)
 - **od_user_homes** (MD5: 5e56553e863563a662752de9cf98be48) Arguments: /usr/libexec/od_user_homes .localized
 - **cleanup**

Yara Signatures

 No yara matches

Snort Signatures

 No Snort rule has matched

Joe Sandbox Signatures

There are no malicious signatures, [click here to show all signatures](#).

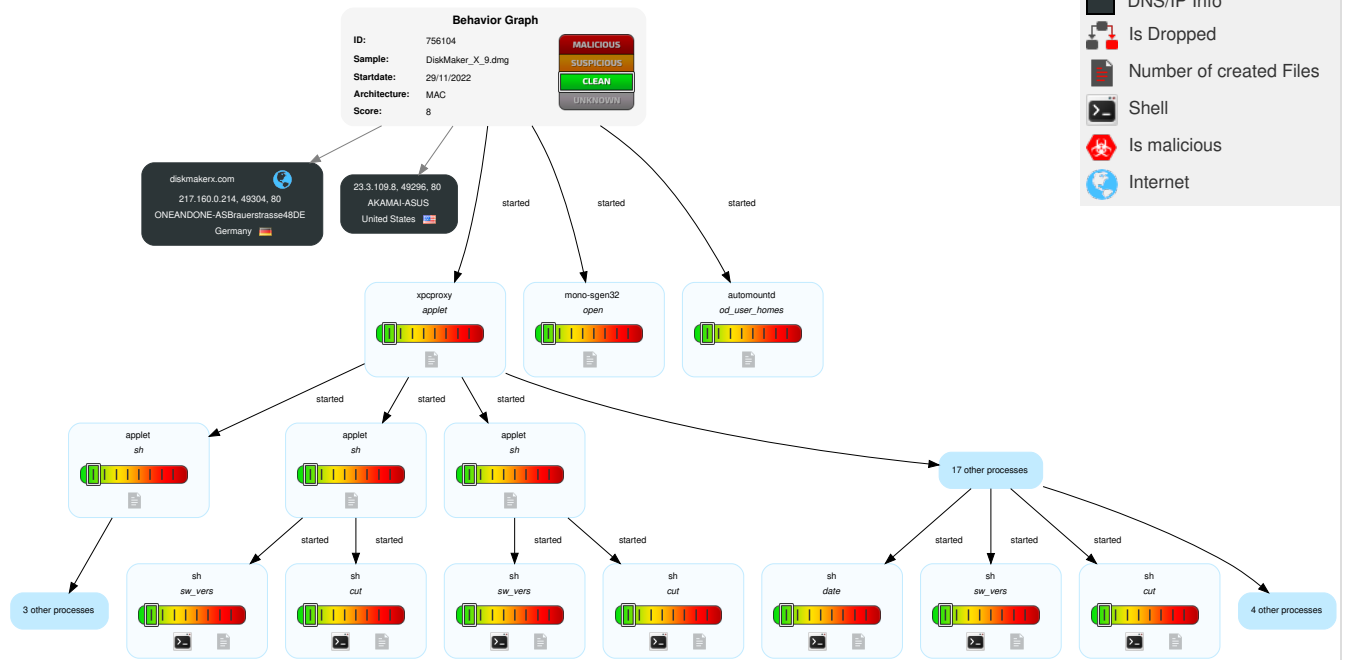
Mitre Att&ck Matrix

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	 Command and Scripting Interpreter	Path Interception	Path Interception	 Scripting	OS Credential Dumping	 Process Discovery	Remote Services	Data from Local System	 Exfiltration Over Alternative Protocol	 Non-Application Layer Protocol	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	 Scripting	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	 Invalid Code Signature	LSASS Memory	  System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	 AppleScript	Logon Script (Windows)	Logon Script (Windows)	 Code Signing	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	 Indicator Removal on Host	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

Behavior Graph

Legend:

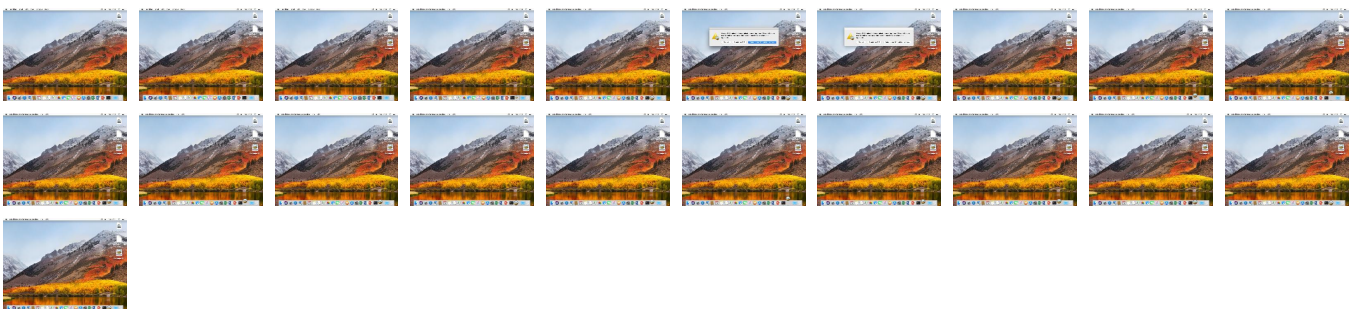
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Number of created Files
- Shell
- Is malicious
- Internet



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DiskMaker_X_9.dmg	0%	Virustotal		Browse
DiskMaker_X_9.dmg	0%	ReversingLabs		

Dropped Files

⊘ No Antivirus matches

Domains

⊘ No Antivirus matches

URLs

⊘ No Antivirus matches

Domains and IPs

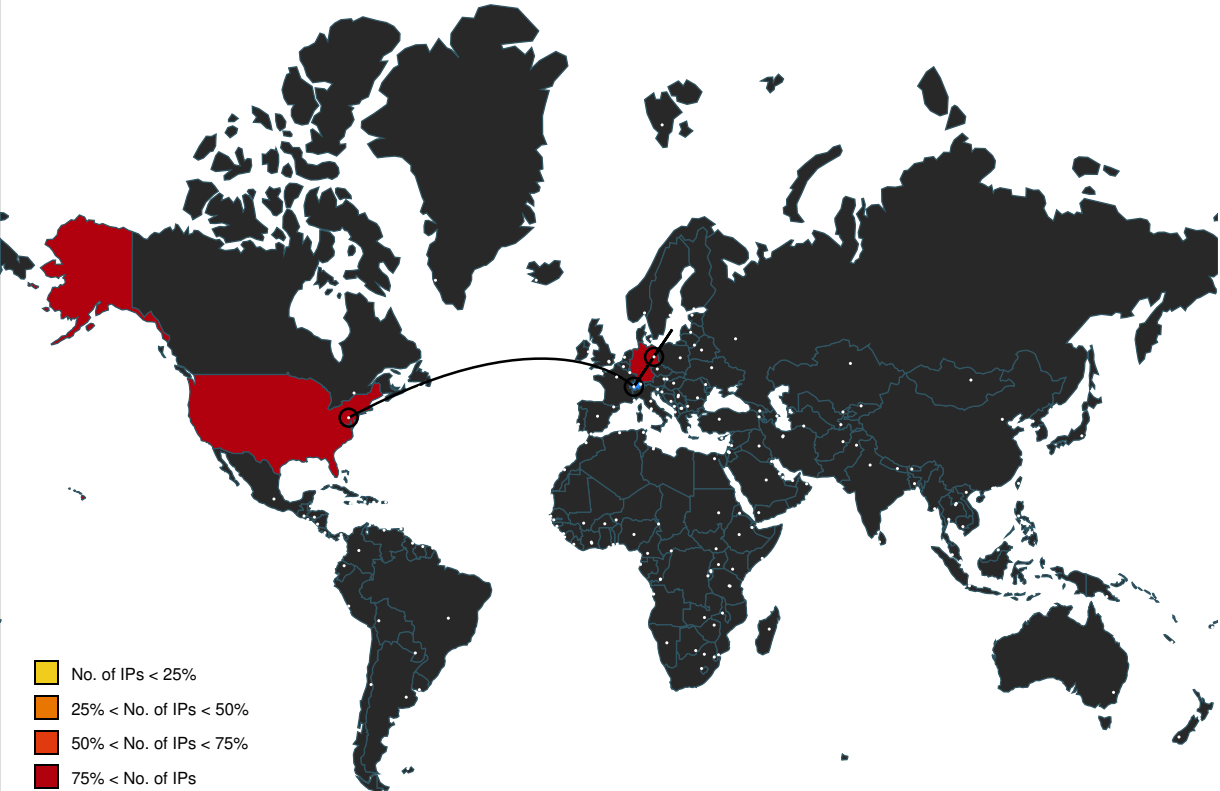
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
diskmakerx.com	217.160.0.214	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://diskmakerx.com/CurrentLDMVersion	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.160.0.214	diskmakerx.com	Germany		8560	ONEANDONE-ASBraucherstrasse48DE	false
23.3.109.8	unknown	United States		16625	AKAMAI-ASUS	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

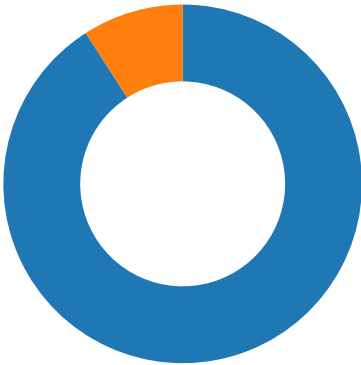
No context

Dropped Files	—
 No context	

Created / dropped Files	—
/Users/berri/Library/Logs/DiskMakerX.log	▼
/dev/null	▼

Static File Info	—
General	—
File type:	bzip2 compressed data, block size = 100k
Entropy (8bit):	7.999667829376183
TrID:	- Disk Image (Macintosh), bzip2 (12509/2) 80.61% - bzip2 compressed archive (3009/2) 19.39%
File name:	DiskMaker_X_9.dmg
File size:	6272758
MD5:	d575c6a40278340f092a6fc4e26e4d11
SHA1:	87d92610155135621014afefa88d8b6c9ad5f0ed
SHA256:	96845cd375543401b822fb4e17d2ecc300cb621f56afcdad613ae11c9afddce
SHA512:	f18cf8eee40b9c1cfe1a2141ffd6e59e36f34fb7908ffb5383847b45bc0b5571efd4c80c2969409744274c744e6124dd3d2a62d408501d71ceb8bab7f4585d3f
SSDEEP:	98304:SqTiPyIC9pzheDyGVPAJBajolz82jt58wb9TmzV4C1V5zw7NSmj5TGdjFOIZRZ/d:fTiaPpAVPAJwA68wb9adjwgiFG5F7PZq
TLSH:	F95633367A1CFC39EC61DA7657CB827FEF5B29C38A52534029766B81077B3A42B31460
File Content Preview:	BZh11AY&SY...[...G.....@...1....%.....H.....`BZh11AY&SY"4e.....P.@....BH.....@...u..2....i.6..P....Tq.w.&...8....H....F#.X.Ou.....-.....@.?....cN&..K@./...N.\$...~@BZh91AY&SYTtL...e.....R(+..=.....yuA.

CodeSign Information	▼
-----------------------------	---

Network Behavior	—
Network Port Distribution	—
 Total Packets: 11 53 (DNS) 80 (HTTP)	

TCP Packets	▼
UDP Packets	▼
ICMP Packets	▼

DNS Queries								
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 16:39:51.757548094 CET	192.168.11.11	1.1.1.1	0x6cf2	Standard query (0)	diskmakerx.com	A (IP address)	IN (0x0001)	false

DNS Answers										
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 16:39:51.778717041 CET	1.1.1.1	192.168.11.11	0x6cf2	No error (0)	diskmakerx.com		217.160.0.214	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph										
diskmakerx.com										

System Behavior

Analysis Process: mono-sgen32 PID: 892, Parent PID: 812										
General										
Start time:	16:39:43									
Start date:	29/11/2022									
Path:	/Library/Frameworks/Mono.framework/Versions/4.4.2/bin/mono-sgen32									
Arguments:	n/a									
File size:	3722408 bytes									
MD5 hash:	8910349f44a940d8d79318367855b236									

Analysis Process: open PID: 892, Parent PID: 812										
General										
Start time:	16:39:43									
Start date:	29/11/2022									
Path:	/usr/bin/open									
Arguments:										
File size:	105952 bytes									
MD5 hash:	40ed6d8f35c9f20484b97582d296398f									

File Activities										
File Read										
Directory Enumerated										

Analysis Process: xpcproxy PID: 893, Parent PID: 1										
General										
Start time:	16:39:43									
Start date:	29/11/2022									
Path:	/usr/libexec/xpcproxy									
Arguments:	n/a									
File size:	43488 bytes									
MD5 hash:	d1bb9a4899f0af921e8188218b20d744									

File Activities										
File Read										
Directory Created										

Analysis Process: applet PID: 893, Parent PID: 1		—
General		—
Start time:	16:39:43	
Start date:	29/11/2022	
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet	
Arguments:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet	
File size:	60192 bytes	
MD5 hash:	0717bb720584b8dc860a0b9e235dd447	

File Activities		—
File Read		▼
File Written		▼
Directory Enumerated		▼
Directory Attributes Enumerated Bulk		▼
Directory Created		▼

Analysis Process: applet PID: 894, Parent PID: 893		—
General		—
Start time:	16:39:43	
Start date:	29/11/2022	
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet	
Arguments:	n/a	
File size:	60192 bytes	
MD5 hash:	0717bb720584b8dc860a0b9e235dd447	

Analysis Process: sh PID: 894, Parent PID: 893		—
General		—
Start time:	16:39:44	
Start date:	29/11/2022	
Path:	/bin/sh	
Arguments:	sh -c echo \$HOME	
File size:	618512 bytes	
MD5 hash:	8aa60b22a5d30418a002b340989384dc	

File Activities		—
File Read		▼

Analysis Process: applet PID: 895, Parent PID: 893		—
General		—
Start time:	16:39:44	
Start date:	29/11/2022	
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet	
Arguments:	n/a	
File size:	60192 bytes	
MD5 hash:	0717bb720584b8dc860a0b9e235dd447	

Analysis Process: sh PID: 895, Parent PID: 893		—
General		—
Start time:	16:39:44	
Start date:	29/11/2022	
Path:	/bin/sh	
Arguments:	sh -c touch '/Users/berri/Library/Logs/DiskMakerX.log	
File size:	618512 bytes	
MD5 hash:	8aa60b22a5d30418a002b340989384dc	

File Activities		—
-----------------	--	---

File Read

Analysis Process: touch PID: 895, Parent PID: 893

General	
Start time:	16:39:44
Start date:	29/11/2022
Path:	/usr/bin/touch
Arguments:	touch /Users/berri/Library/Logs/DiskMakerX.log
File size:	23376 bytes
MD5 hash:	4aacabad02929f18b00a9b6ef85e0605

File Activities

File Created

File Read

Analysis Process: applet PID: 896, Parent PID: 893

General	
Start time:	16:39:44
Start date:	29/11/2022
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet
Arguments:	n/a
File size:	60192 bytes
MD5 hash:	0717bb720584b8dc860a0b9e235dd447

Analysis Process: sh PID: 896, Parent PID: 893

General	
Start time:	16:39:44
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	sh -c echo '-----' >> '/Users/berri/Library/Logs/DiskMakerX.log'
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

File Activities

File Read

File Written

Analysis Process: applet PID: 897, Parent PID: 893

General	
Start time:	16:39:44
Start date:	29/11/2022
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet
Arguments:	n/a
File size:	60192 bytes
MD5 hash:	0717bb720584b8dc860a0b9e235dd447

Analysis Process: sh PID: 897, Parent PID: 893

General	
Start time:	16:39:44
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	sh -c date >> '/Users/berri/Library/Logs/DiskMakerX.log'
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

File Activities

File Read

Analysis Process: sh PID: 898, Parent PID: 897

General	
Start time:	16:39:44
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	n/a
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

Analysis Process: date PID: 898, Parent PID: 897

General	
Start time:	16:39:44
Start date:	29/11/2022
Path:	/bin/date
Arguments:	date
File size:	28592 bytes
MD5 hash:	e1d20c480fcdc1ac4646170b1d9ca7c7

File Activities

File Read

File Written

Analysis Process: applet PID: 899, Parent PID: 893

General	
Start time:	16:39:44
Start date:	29/11/2022
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet
Arguments:	n/a
File size:	60192 bytes
MD5 hash:	0717bb720584b8dc860a0b9e235dd447

Analysis Process: sh PID: 899, Parent PID: 893

General	
Start time:	16:39:44
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	sh -c echo 'Home Path: ' '/Users/berri'>> '/Users/berri/Library/Logs/DiskMakerX.log
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

File Activities

File Read

File Written

Analysis Process: applet PID: 900, Parent PID: 893

General	
Start time:	16:39:44
Start date:	29/11/2022
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet
Arguments:	n/a
File size:	60192 bytes
MD5 hash:	0717bb720584b8dc860a0b9e235dd447

Analysis Process: sh PID: 900, Parent PID: 893

General	
Start time:	16:39:44
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	sh -c defaults read NSGlobalDomain AppleLanguages
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

File Activities	
File Read	

Analysis Process: defaults PID: 900, Parent PID: 893	
General	
Start time:	16:39:44
Start date:	29/11/2022
Path:	/usr/bin/defaults
Arguments:	defaults read NSGlobalDomain AppleLanguages
File size:	39472 bytes
MD5 hash:	831678c94c2d9c647bf3d283b1861bda

File Activities	
File Read	
Directory Enumerated	

Analysis Process: applet PID: 901, Parent PID: 893	
General	
Start time:	16:39:50
Start date:	29/11/2022
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet
Arguments:	n/a
File size:	60192 bytes
MD5 hash:	0717bb720584b8dc860a0b9e235dd447

Analysis Process: sh PID: 901, Parent PID: 893	
General	
Start time:	16:39:50
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	sh -c echo 'Current Language: ' en-CH>> '/Users/berri/Library/Logs/DiskMakerX.log
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

File Activities	
File Read	
File Written	

Analysis Process: applet PID: 902, Parent PID: 893	
General	
Start time:	16:39:50
Start date:	29/11/2022
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet
Arguments:	n/a
File size:	60192 bytes
MD5 hash:	0717bb720584b8dc860a0b9e235dd447

Analysis Process: sh PID: 902, Parent PID: 893	
--	--

General	
Start time:	16:39:50
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	sh -c sw_vers -productVersion cut -c 1-4
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

File Activities	
File Read	

Analysis Process: sh PID: 903, Parent PID: 902	
General	
Start time:	16:39:50
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	n/a
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

Analysis Process: sw_vers PID: 903, Parent PID: 902	
General	
Start time:	16:39:50
Start date:	29/11/2022
Path:	/usr/bin/sw_vers
Arguments:	sw_vers -productVersion
File size:	18848 bytes
MD5 hash:	d33f7f9efd4158694d0d58879b54f89d

File Activities	
File Read	
Directory Enumerated	

Analysis Process: sh PID: 904, Parent PID: 902	
General	
Start time:	16:39:50
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	n/a
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

Analysis Process: cut PID: 904, Parent PID: 902	
General	
Start time:	16:39:50
Start date:	29/11/2022
Path:	/usr/bin/cut
Arguments:	cut -c 1-4
File size:	23712 bytes
MD5 hash:	e27c92637d672468ea846d377b500eb1

File Activities	
File Read	

Analysis Process: applet PID: 905, Parent PID: 893	
General	

Start time:	16:39:50
Start date:	29/11/2022
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet
Arguments:	n/a
File size:	60192 bytes
MD5 hash:	0717bb720584b8dc860a0b9e235dd447

Analysis Process: sh PID: 905, Parent PID: 893

General

Start time:	16:39:50
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	sh -c sw_vers -productVersion cut -c 4-4
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

File Activities

File Read

Analysis Process: sh PID: 906, Parent PID: 905

General

Start time:	16:39:50
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	n/a
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

Analysis Process: sw_vers PID: 906, Parent PID: 905

General

Start time:	16:39:50
Start date:	29/11/2022
Path:	/usr/bin/sw_vers
Arguments:	sw_vers -productVersion
File size:	18848 bytes
MD5 hash:	d33f7f9efd4158694d0d58879b54f89d

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 907, Parent PID: 905

General

Start time:	16:39:50
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	n/a
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

Analysis Process: cut PID: 907, Parent PID: 905

General

Start time:	16:39:50
Start date:	29/11/2022
Path:	/usr/bin/cut
Arguments:	cut -c 4-4

File size:	23712 bytes
MD5 hash:	e27c92637d672468ea846d377b500eb1

File Activities	—
File Read	▼

Analysis Process: applet	PID: 908, Parent PID: 893	—
General		—
Start time:	16:39:50	
Start date:	29/11/2022	
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet	
Arguments:	n/a	
File size:	60192 bytes	
MD5 hash:	0717bb720584b8dc860a0b9e235dd447	

Analysis Process: sh	PID: 908, Parent PID: 893	—
General		—
Start time:	16:39:50	
Start date:	29/11/2022	
Path:	/bin/sh	
Arguments:	sh -c sw_vers -productVersion cut -c 1-5	
File size:	618512 bytes	
MD5 hash:	8aa60b22a5d30418a002b340989384dc	

File Activities	—
File Read	▼

Analysis Process: sh	PID: 909, Parent PID: 908	—
General		—
Start time:	16:39:50	
Start date:	29/11/2022	
Path:	/bin/sh	
Arguments:	n/a	
File size:	618512 bytes	
MD5 hash:	8aa60b22a5d30418a002b340989384dc	

Analysis Process: sw_vers	PID: 909, Parent PID: 908	—
General		—
Start time:	16:39:50	
Start date:	29/11/2022	
Path:	/usr/bin/sw_vers	
Arguments:	sw_vers -productVersion	
File size:	18848 bytes	
MD5 hash:	d33f7f9efd4158694d0d58879b54f89d	

File Activities	—
File Read	▼
Directory Enumerated	▼

Analysis Process: sh	PID: 910, Parent PID: 908	—
General		—
Start time:	16:39:50	
Start date:	29/11/2022	
Path:	/bin/sh	
Arguments:	n/a	
File size:	618512 bytes	

MD5 hash:	8aa60b22a5d30418a002b340989384dc
-----------	----------------------------------

Analysis Process: cut PID: 910, Parent PID: 908		—
General		—
Start time:	16:39:50	
Start date:	29/11/2022	
Path:	/usr/bin/cut	
Arguments:	cut -c 1-5	
File size:	23712 bytes	
MD5 hash:	e27c92637d672468ea846d377b500eb1	

File Activities	—
File Read	▼

Analysis Process: applet PID: 911, Parent PID: 893		—
General		—
Start time:	16:39:50	
Start date:	29/11/2022	
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet	
Arguments:	n/a	
File size:	60192 bytes	
MD5 hash:	0717bb720584b8dc860a0b9e235dd447	

Analysis Process: sh PID: 911, Parent PID: 893		—
General		—
Start time:	16:39:50	
Start date:	29/11/2022	
Path:	/bin/sh	
Arguments:	sh -c sw_vers -productVersion cut -c 4-5	
File size:	618512 bytes	
MD5 hash:	8aa60b22a5d30418a002b340989384dc	

File Activities	—
File Read	▼

Analysis Process: sh PID: 912, Parent PID: 911		—
General		—
Start time:	16:39:50	
Start date:	29/11/2022	
Path:	/bin/sh	
Arguments:	n/a	
File size:	618512 bytes	
MD5 hash:	8aa60b22a5d30418a002b340989384dc	

Analysis Process: sw_vers PID: 912, Parent PID: 911		—
General		—
Start time:	16:39:50	
Start date:	29/11/2022	
Path:	/usr/bin/sw_vers	
Arguments:	sw_vers -productVersion	
File size:	18848 bytes	
MD5 hash:	d33f7f9efd4158694d0d58879b54f89d	

File Activities	—
File Read	▼
Directory Enumerated	▼

Analysis Process: sh PID: 913, Parent PID: 911		—
General		—
Start time:	16:39:50	
Start date:	29/11/2022	
Path:	/bin/sh	
Arguments:	n/a	
File size:	618512 bytes	
MD5 hash:	8aa60b22a5d30418a002b340989384dc	

Analysis Process: cut PID: 913, Parent PID: 911		—
General		—
Start time:	16:39:50	
Start date:	29/11/2022	
Path:	/usr/bin/cut	
Arguments:	cut -c 4-5	
File size:	23712 bytes	
MD5 hash:	e27c92637d672468ea846d377b500eb1	

File Activities		—
File Read		▼

Analysis Process: applet PID: 914, Parent PID: 893		—
General		—
Start time:	16:39:50	
Start date:	29/11/2022	
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet	
Arguments:	n/a	
File size:	60192 bytes	
MD5 hash:	0717bb720584b8dc860a0b9e235dd447	

Analysis Process: sh PID: 914, Parent PID: 893		—
General		—
Start time:	16:39:50	
Start date:	29/11/2022	
Path:	/bin/sh	
Arguments:	sh -c echo 'Current OS: ' 10.13>> '/Users/berri/Library/Logs/DiskMakerX.log	
File size:	618512 bytes	
MD5 hash:	8aa60b22a5d30418a002b340989384dc	

File Activities		—
File Read		▼
File Written		▼

Analysis Process: applet PID: 915, Parent PID: 893		—
General		—
Start time:	16:39:50	
Start date:	29/11/2022	
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet	
Arguments:	n/a	
File size:	60192 bytes	
MD5 hash:	0717bb720584b8dc860a0b9e235dd447	

Analysis Process: sh PID: 915, Parent PID: 893		—
General		—
Start time:	16:39:50	

Start date:	29/11/2022
Path:	/bin/sh
Arguments:	sh -c id -G
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

File Activities

File Read

Analysis Process: id PID: 915, Parent PID: 893

General

Start time:	16:39:50
Start date:	29/11/2022
Path:	/usr/bin/id
Arguments:	id -G
File size:	23248 bytes
MD5 hash:	24c45eb23e1aae68c572939d1a906018

File Activities

File Read

Analysis Process: applet PID: 916, Parent PID: 893

General

Start time:	16:39:50
Start date:	29/11/2022
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet
Arguments:	n/a
File size:	60192 bytes
MD5 hash:	0717bb720584b8dc860a0b9e235dd447

Analysis Process: sh PID: 916, Parent PID: 893

General

Start time:	16:39:50
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	sh -c echo 'Is this user an admin : ' true>> '/Users/berri/Library/Logs/DiskMakerX.log
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

File Activities

File Read

File Written

Analysis Process: applet PID: 917, Parent PID: 893

General

Start time:	16:39:50
Start date:	29/11/2022
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet
Arguments:	n/a
File size:	60192 bytes
MD5 hash:	0717bb720584b8dc860a0b9e235dd447

Analysis Process: sh PID: 917, Parent PID: 893

General

Start time:	16:39:50
Start date:	29/11/2022

Path:	/bin/sh
Arguments:	sh -c ps auxc
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

File Activities	—
File Read	▼

Analysis Process: ps	PID: 917, Parent PID: 893	—
General	—	
Start time:	16:39:50	
Start date:	29/11/2022	
Path:	/bin/ps	
Arguments:	ps auxc	
File size:	51280 bytes	
MD5 hash:	792e18b1417ac1f184680d2423206e4f	

File Activities	—
File Read	▼
Directory Enumerated	▼

Analysis Process: applet	PID: 918, Parent PID: 893	—
General	—	
Start time:	16:39:51	
Start date:	29/11/2022	
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet	
Arguments:	n/a	
File size:	60192 bytes	
MD5 hash:	0717bb720584b8dc860a0b9e235dd447	

Analysis Process: sh	PID: 918, Parent PID: 893	—
General	—	
Start time:	16:39:51	
Start date:	29/11/2022	
Path:	/bin/sh	
Arguments:	sh -c echo 'Path Finder launched : ' false>> '/Users/berri/Library/Logs/DiskMakerX.log	
File size:	618512 bytes	
MD5 hash:	8aa60b22a5d30418a002b340989384dc	

File Activities	—
File Read	▼
File Written	▼

Analysis Process: applet	PID: 919, Parent PID: 893	—
General	—	
Start time:	16:39:51	
Start date:	29/11/2022	
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet	
Arguments:	n/a	
File size:	60192 bytes	
MD5 hash:	0717bb720584b8dc860a0b9e235dd447	

Analysis Process: sh	PID: 919, Parent PID: 893	—
General	—	
Start time:	16:39:51	
Start date:	29/11/2022	

Path:	/bin/sh
Arguments:	sh -c curl http://diskmakerx.com/CurrentLDMVersion
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

File Activities	—
File Read	▼

Analysis Process: curl	PID: 919, Parent PID: 893	—
General	—	
Start time:	16:39:51	
Start date:	29/11/2022	
Path:	/usr/bin/curl	
Arguments:	curl http://diskmakerx.com/CurrentLDMVersion	
File size:	185104 bytes	
MD5 hash:	078cd73f58d3d8f875eed22522ff73f7	

File Activities	—
File Read	▼

Analysis Process: applet	PID: 920, Parent PID: 893	—
General	—	
Start time:	16:39:51	
Start date:	29/11/2022	
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet	
Arguments:	n/a	
File size:	60192 bytes	
MD5 hash:	0717bb720584b8dc860a0b9e235dd447	

Analysis Process: sh	PID: 920, Parent PID: 893	—
General	—	
Start time:	16:39:51	
Start date:	29/11/2022	
Path:	/bin/sh	
Arguments:	sh -c echo 'Selected OS: ' 10.15>> '/Users/berri/Library/Logs/DiskMakerX.log	
File size:	618512 bytes	
MD5 hash:	8aa60b22a5d30418a002b340989384dc	

File Activities	—
File Read	▼
File Written	▼

Analysis Process: applet	PID: 921, Parent PID: 893	—
General	—	
Start time:	16:39:57	
Start date:	29/11/2022	
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet	
Arguments:	n/a	
File size:	60192 bytes	
MD5 hash:	0717bb720584b8dc860a0b9e235dd447	

Analysis Process: sh	PID: 921, Parent PID: 893	—
General	—	
Start time:	16:39:57	
Start date:	29/11/2022	
Path:	/bin/sh	

Arguments:	sh -c mdfind -name 'Install macOS Catalina' grep -v Library head -1
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

File Activities

File Read

Analysis Process: sh PID: 922, Parent PID: 921

General

Start time:	16:39:57
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	n/a
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

Analysis Process: mdfind PID: 922, Parent PID: 921

General

Start time:	16:39:57
Start date:	29/11/2022
Path:	/usr/bin/mdfind
Arguments:	mdfind -name Install macOS Catalina
File size:	29280 bytes
MD5 hash:	84f3a3da590e65271df7fecb27671fac

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 923, Parent PID: 921

General

Start time:	16:39:57
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	n/a
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

Analysis Process: grep PID: 923, Parent PID: 921

General

Start time:	16:39:57
Start date:	29/11/2022
Path:	/usr/bin/grep
Arguments:	grep -v Library
File size:	33936 bytes
MD5 hash:	2b3efb273296881708ea2914c612e0eb

File Activities

File Read

Analysis Process: sh PID: 924, Parent PID: 921

General

Start time:	16:39:57
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	n/a

File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

Analysis Process: head PID: 924, Parent PID: 921	
General	
Start time:	16:39:57
Start date:	29/11/2022
Path:	/usr/bin/head
Arguments:	head -1
File size:	18912 bytes
MD5 hash:	bb2984cc21ccc7343bed41f2b577c011

File Activities	
File Read	

Analysis Process: applet PID: 925, Parent PID: 893	
General	
Start time:	16:39:57
Start date:	29/11/2022
Path:	/Volumes/DiskMaker X 9/DiskMaker X 9 for macOS Catalina.app/Contents/MacOS/applet
Arguments:	n/a
File size:	60192 bytes
MD5 hash:	0717bb720584b8dc860a0b9e235dd447

Analysis Process: sh PID: 925, Parent PID: 893	
General	
Start time:	16:39:57
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	sh -c echo " wc -l
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

File Activities	
File Read	

Analysis Process: sh PID: 926, Parent PID: 925	
General	
Start time:	16:39:57
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	n/a
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

Analysis Process: sh PID: 927, Parent PID: 925	
General	
Start time:	16:39:57
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	n/a
File size:	618512 bytes
MD5 hash:	8aa60b22a5d30418a002b340989384dc

Analysis Process: wc PID: 927, Parent PID: 925	
General	

Start time:	16:39:57
Start date:	29/11/2022
Path:	/usr/bin/wc
Arguments:	wc -l
File size:	23072 bytes
MD5 hash:	b89949ce6a1929257e5c0c157027cbfe

File Activities

File Read

Analysis Process: automountd PID: 928, Parent PID: 837

General

Start time:	16:40:01
Start date:	29/11/2022
Path:	/usr/libexec/automountd
Arguments:	n/a
File size:	129632 bytes
MD5 hash:	a02648ba58feca82fec051bdd78be4b6

Analysis Process: od_user_homes PID: 928, Parent PID: 837

General

Start time:	16:40:01
Start date:	29/11/2022
Path:	/usr/libexec/od_user_homes
Arguments:	/usr/libexec/od_user_homes .localized
File size:	24656 bytes
MD5 hash:	5e56553e863563a662752de9cf98be48

File Activities

File Read