Sep 12 2023

NETMANAGEIT

Intelligence Report

Free Download Manager backdoored, a possible supply chain attack on Linux machines

Table of contents

Overview

- Description 4
- Confidence 4

Entities

- Indicator 5
- Attack-Pattern 11

Observables

- Domain-Name 12
- StixFile 13
- Hostname 14
- IPv4-Addr 15
- Url 16

External References

- External References 17

Overview

Description

Kaspersky researchers analyzed a Linux backdoor disguised as Free Download Manager software that remained under the radar for at least three years.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Indicator

Name
2c9bf1811ff428ef9ec999cc7544b43950947b0f.u.fdmpkg.org
Pattern Type
stix
Pattern
[hostname:value = '2c9bf1811ff428ef9ec999cc7544b43950947b0f.u.fdmpkg.org']
Name
5d6167ef729c91662badef0950f795bf362cbb99.u.fdmpkg.org
Pattern Type
stix
Pattern
[hostname:value = '5d6167ef729c91662badef0950f795bf362cbb99.u.fdmpkg.org']
Name
fdmpkg.org

Pattern Type
stix
Pattern
[domain-name:value = 'fdmpkg.org']
Name
https://deb.fdmpkg.org/freedownloadmanager.deb
Pattern Type
stix
Pattern
[url:value = 'https://deb.fdmpkg.org/freedownloadmanager.deb']
Name
b77f63f14d0b2bde3f4f62f4323aad87194da11d71c117a487e18ff3f2cd468d
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b77f63f14d0b2bde3f4f62f4323aad87194da11d71c117a487e18ff3f2cd468d']
Name

c6d76b1748b67fbc21ab493281dd1c7a558e3047.u.fdmpkg.org

Pattern Type

stix

Pattern

[hostname:value = 'c6d76b1748b67fbc21ab493281dd1c7a558e3047.u.fdmpkg.org']

Name

93358bfb6ee0caced889e94cd82f6f417965087203ca9a5fce8dc7f6e1b8a3ea

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '93358bfb6ee0caced889e94cd82f6f417965087203ca9a5fce8dc7f6e1b8a3ea']

Name

0727bedf5c1f85f58337798a63812aa986448473.u.fdmpkg.org

Pattern Type

stix

Pattern

[hostname:value = '0727bedf5c1f85f58337798a63812aa986448473.u.fdmpkg.org']

Name

d73be6e13732d365412d71791e5eb1096c7bb13d6f7fd533d8c04392ca0b69b5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd73be6e13732d365412d71791e5eb1096c7bb13d6f7fd533d8c04392ca0b69b5']

Name

deb.fdmpkg.org

Pattern Type

stix

Pattern

[hostname:value = 'deb.fdmpkg.org']

Name

172.111.48.101

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.111.48.101']

Name

172.1.0.80

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.1.0.80']

Name

2214c7a0256f07ce7b7aab8f61ef9cbaff10a456c8b9f2a97d8f713abd660349

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2214c7a0256f07ce7b7aab8f61ef9cbaff10a456c8b9f2a97d8f713abd660349']

Name

c3a05f0dac05669765800471abc1fdaba15e3360.u.fdmpkg.org

Pattern Type

stix

Pattern
[hostname:value = 'c3a05f0dac05669765800471abc1fdaba15e3360.u.fdmpkg.org']

Attack-Pattern

Name
Supply Chain Compromise
ID
T1195
Description
Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: * Manipulation of development tools * Manipulation of a development environment * Manipulation of source code repositories (public or private) * Manipulation of source code in open-source dependencies * Manipulation of software update/distribution mechanisms * Compromised/infected system images (multiple cases of removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware) * Replacement of legitimate software with modified versions * Sales of modified/counterfeit products to legitimate distributors * Shipment interdiction While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

Domain-Name

Value
fdmpkg.org

StixFile

Value
d73be6e13732d365412d71791e5eb1096c7bb13d6f7fd533d8c04392ca0b69b5
93358bfb6ee0caced889e94cd82f6f417965087203ca9a5fce8dc7f6e1b8a3ea
2214c7a0256f07ce7b7aab8f61ef9cbaff10a456c8b9f2a97d8f713abd660349
b77f63f14d0b2bde3f4f62f4323aad87194da11d71c117a487e18ff3f2cd468d

Hostname

Value
0727bedf5c1f85f58337798a63812aa986448473.u.fdmpkg.org
c3a05f0dac05669765800471abc1fdaba15e3360.u.fdmpkg.org
5d6167ef729c91662badef0950f795bf362cbb99.u.fdmpkg.org
c6d76b1748b67fbc21ab493281dd1c7a558e3047.u.fdmpkg.org
deb.fdmpkg.org
2c9bf1811ff428ef9ec999cc7544b43950947b0f.u.fdmpkg.org

IPv4-Addr

Value
172.1.0.80
172.111.48.101

Url

Value
https://deb.fdmpkg.org/freedownloadmanager.deb

External References

- https://otx.alienvault.com/pulse/650082e658c511d14275e5bc
- https://securelist.com/backdoored-free-download-manager-linux-malware/110465/