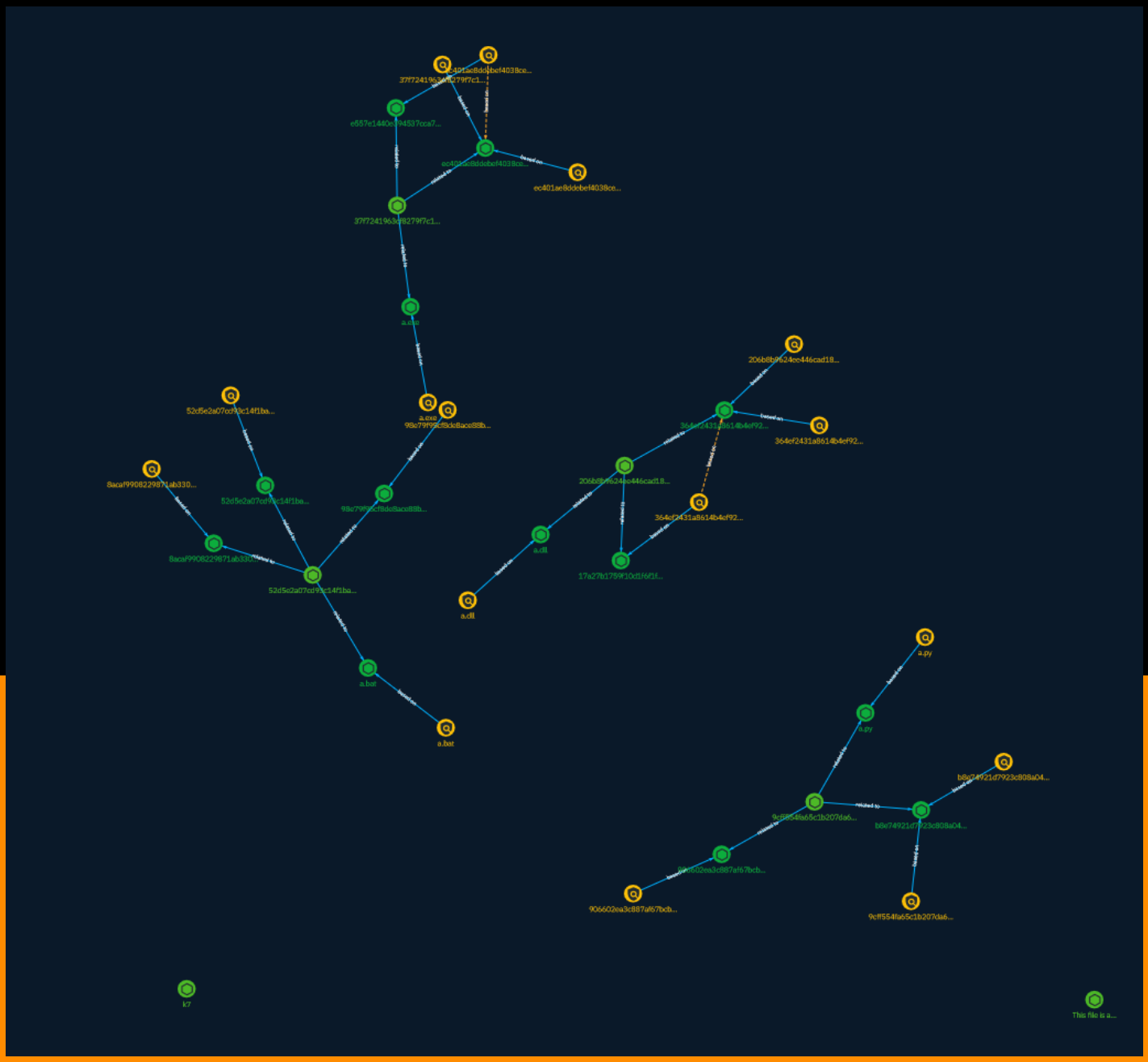
Dec 06 2023

NETMANAGEIT

# Intelligence Report

# MAR-10478915-1.v1 Citrix Bleed



# Table of contents

## Overview



## Entities



## Observables



## External References

# Overview

## Description

MAR-10478915-1.v1 Citrix Bleed

## Confidence

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

20 / 100

# Content

N/A

# Indicator

| Name |
| --- |
| 98e79f95cf8de8ace88bf223421db5dce303b112152d66ffdf27ebdfcdf967e9 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = '98e79f95cf8de8ace88bf223421db5dce303b112152d66ffdf27ebdfcdf967e9'] |
| **Name** |
| ec401ae8ddebef4038cedb65cc0d5ba6c1fdef28 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-1' = 'ec401ae8ddebef4038cedb65cc0d5ba6c1fdef28'] |
| **Name** |

a.exe

**Pattern Type**

stix

**Pattern**

[file:name = 'a.exe']

**Name**

a.bat

**Pattern Type**

stix

**Pattern**

[file:name = 'a.bat']

**Name**

906602ea3c887af67bcb4531bbbb459d7c24a2efcb866bcb1e3b028a51f12ae6

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '906602ea3c887af67bcb4531bbbb459d7c24a2efcb866bcb1e3b028a51f12ae6']

| Name |
| --- |
| 52d5e2a07cd93c14f1ba170e3a3d6747 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.MD5 = '52d5e2a07cd93c14f1ba170e3a3d6747'] |
| **Name** |
| 364ef2431a8614b4ef9240afa00cd12bfba3119b |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-1' = '364ef2431a8614b4ef9240afa00cd12bfba3119b'] |
| **Name** |
| 37f7241963cf8279f7c1d322086a5194 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.MD5 = '37f7241963cf8279f7c1d322086a5194'] |

| Name |
| --- |
| b8e74921d7923c808a0423e6e46807c4f0699b6e |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-1' = 'b8e74921d7923c808a0423e6e46807c4f0699b6e'] |
| **Name** |
| 9cff554fa65c1b207da66683b295d4ad |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.MD5 = '9cff554fa65c1b207da66683b295d4ad'] |
| **Name** |
| ec401ae8ddebef4038cedb65cc0d5ba6c1fdef28 |
| **Description** |
| Created by VirusTotal connector as the positive count was >= 10 |
| **Pattern Type** |
| stix |

**Pattern**

[file:hashes.'SHA-256' = 'e557e1440e394537cca71ed3d61372106c3c70eb6ef9f07521768f23a0974068']

**Name**

a.dll

**Pattern Type**

stix

**Pattern**

[file:name = 'a.dll']

**Name**

8acaf9908229871ab33033df7b6a328ec1db56d5

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-1' = '8acaf9908229871ab33033df7b6a328ec1db56d5']

**Name**

206b8b9624ee446cad18335702d6da19

**Pattern Type**

stix

**Pattern**

[file:hashes.MD5 = '206b8b9624ee446cad18335702d6da19']

**Name**

364ef2431a8614b4ef9240afa00cd12bfba3119b

**Description**

Created by VirusTotal connector as the positive count was >= 10

**Pattern Type**

stix

**Pattern**

[file:hashes.'SHA-256' = '17a27b1759f10d1f6f1f51a11c0efea550e2075c2c394259af4d3f855bbcc994']

**Name**

a.py

**Pattern Type**

stix

**Pattern**

[file:name = 'a.py']

# StixFile

| Value |
| --- |
| 8acaf9908229871ab33033df7b6a328ec1db56d5 |
| 906602ea3c887af67bcb4531bbbb459d7c24a2efcb866bcb1e3b028a51f12ae6 |
| ec401ae8ddebef4038cedb65cc0d5ba6c1fdef28 |
| b8e74921d7923c808a0423e6e46807c4f0699b6e |
| e557e1440e394537cca71ed3d61372106c3c70eb6ef9f07521768f23a0974068 |
| a.py |
| 17a27b1759f10d1f6f1f51a11c0efea550e2075c2c394259af4d3f855bbcc994 |
| 98e79f95cf8de8ace88bf223421db5dce303b112152d66ffdf27ebdfcdf967e9 |
| a.bat |
| a.dll |
| 364ef2431a8614b4ef9240afa00cd12bfba3119b |
| a.exe |
| 52d5e2a07cd93c14f1ba170e3a3d6747 |

# Text

| Value |
| --- |
| avira |
| 37f7241963cf8279f7c1d322086a5194 |
| emsisoft |
| 9cff554fa65c1b207da66683b295d4ad |
| 206b8b9624ee446cad18335702d6da19 |
| zillya |
| k7 |
| bitdefender |
| This file is a 64-bit Windows DLL called a.dll that is executed by a.bat as a parameter for the file a.exe. The file a.exe loads this file into the running LSASS process on the infected machine. The file a.dll calls the Windows API CreateFileW to create a file called a.png in the path %PUBLIC%\ Next, a.dll loads DbgCore.dll then utilizes MiniDumpWriteDump function to dump LSASS process memory to disk. If successful, the dumped process memory is written to a.png. Once this is complete, the file a.bat specifies that the file a.png is used to create the cabinet file called a.cab in the path %WINDIR%\Tasks. |
| antiy |

| |
|---|
| ikarus |
| MAR-10478915.r1.v1.CLEAR_stix2.json |
| eset |
| https://www.cisa.gov/news-events/analysis-reports/ar23-325a |
| 52d5e2a07cd93c14f1ba170e3a3d6747 |

This file is a 64-bit Windows command-line executable called a.exe that is executed by a.bat. This file issues the Remote Procedure Call (RPC) ncalrpc:[lsasspirpc] to the RPC end point to provide a file path to the LSASS on the infected machine. Once the file path is returned, the malware loads the accompanying DLL file called a.dll into the running LSASS process. If the DLL is correctly loaded, then the malware outputs the message "[*]success" in the console.

# External References

- http://opencti:8080/storage/get/import/Report/fe4517a1-e28e-45fb-8630-5385e92c33f3/MAR-10478915.r1.v1.CLEAR_.pdf