Akamai ETP Static Analysis Report

© Akamai Technologies, Inc.

Part I. Analysis Overview

Summary

ID	403229d4f0895c21cf913cf127e14135130672b3e23a5e813c208d60a0a46bae.file
Processing End Timestamp	2020-04-28T15:45:28Z
Processing Start Timestamp	2020-04-28T15:45:24Z
Scan Start Timestamp	2020-04-28T15:45:24Z
Scan End Timestamp	2020-04-28T15:45:28Z
Scan Time	4.38 Seconds
Size	73.40 MB
Source Timestamp	2020-04-28T15:45:24Z
Type	Microsoft OOXML Excel 2007+

Malicious Streams

This is the data(matched data streams) that the scan detected is malicious.

VBA/source.vba

Tags

Malicious_Macro, Macro

Part II. Matched Streams

Stream Name: 403229d4f0895c21cf913cf127e14135130672b3e23a5e813c208d60a0a46bae.file

Result	CLEAN
Name	403229d4f0895c21cf913cf127e14135130672b3e23a5e813c208d60a0a46bae.file
Depth	0
Size	73.400 MB
Detected File	true
Type	Microsoft OOXML Excel 2007+
Hash	403229d4f0895c21cf913cf127e14135130672b3e23a5e813c208d60a0a46bae

Matched Stream Details:

Tags

Macro

Stream Name: VBA/source.vba

Result	MALICIOUS
Name	VBA/source.vba
Depth	2
Size	0.909 KB
Detected File	false
Type	VBA macro
Hash	e69073b56b6544c9f6862e2edcae4f81df05d0f3dc71efd28e3327bd02487d6b

Matched Stream Details:

Assembly Details :

Details 1:

Original Code In Line 28:

Shell ("/tmp/_foo_blah")

Evidence:

DropAndExecute

Explanation:

The macro script drops a file on the host and then execute it. May be used to drop and execute a malware.

Offset	28
Length	24
Type	Macro

Tags

Macro, Malicious_Macro