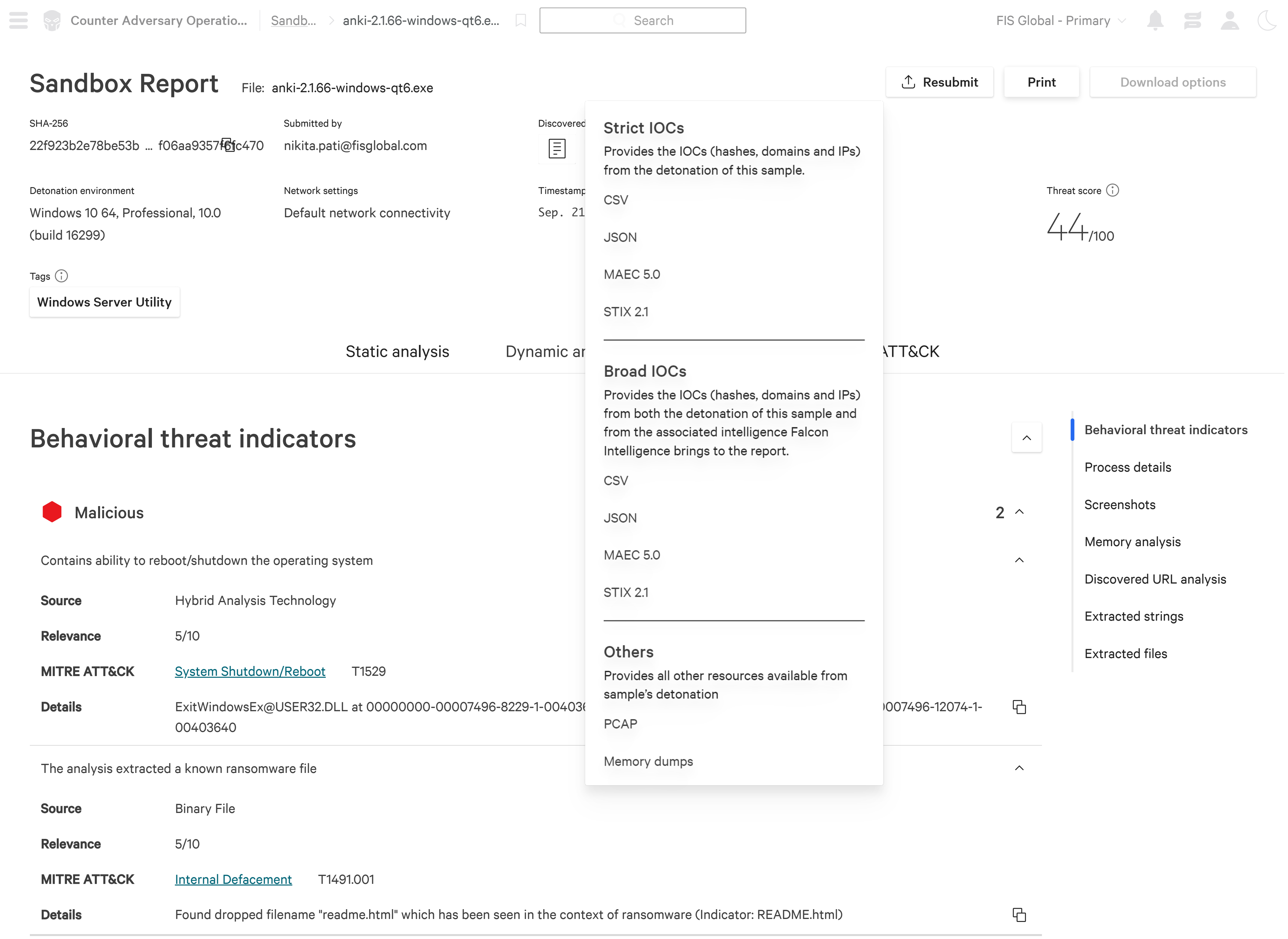


Sandbox Report

File: anki-2.1.66-windows-qt6.exe

SHA-256
22f923b2e78be53b ... f06aa9357f6fc470

Submitted by
nikita.pati@fisglobal.com

Discovered

Detonation environment
Windows 10 64, Professional, 10.0 (build 16299)

Network settings
Default network connectivity

Timestamp
Sep. 21

Threat score
44/100

Tags
Windows Server Utility

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

Behavioral threat indicators

Malicious 2

Contains ability to reboot/shutdown the operating system

Source	Hybrid Analysis Technology
Relevance	5/10
MITRE ATT&CK	System Shutdown/Reboot T1529
Details	ExitWindowsEx@USER32.DLL at 00000000-00007496-8229-1-00403)007496-12074-1-00403640

The analysis extracted a known ransomware file

Source	Binary File
Relevance	5/10
MITRE ATT&CK	Internal Defacement T1491.001
Details	Found dropped filename "readme.html" which has been seen in the context of ransomware (Indicator: README.html)

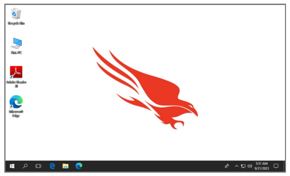
Suspicious 42

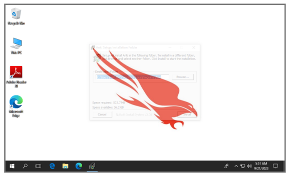
Informative 151

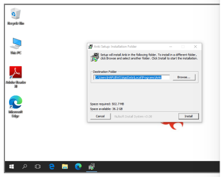
Process details

anki-2.1.66-windows-qt6.exe PID 7496

Screenshots







Memory analysis

Download memory dumps

anki-2.1.66-windows-qt6.exe 9

Discovered URL analysis

No verdict 1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

Extracted strings

Download extracted strings

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

pythonservice.exe	1
win32evtlog.pyd	1
QtPdfWidgets.pyd	1
sip.cp39-win_amd64.pyd	1
axscript.pyd	1
mapi.pyd	1
Qt6QuickTimeline.dll	1
Qt6TextToSpeech.dll	1
QtRemoteObjects.pyd	1
qoffscreen.dll	1
QtSerialPort.pyd	1
QtNfc.pyd	1
_win32sysloader.pyd	1

_speedups.cp39-win_amd64.pyd	1 ⌄
qtsensors_winrt.dll	1 ⌄
qminimal.dll	1 ⌄
quicklintplugin.dll	1 ⌄
qtposition_nmea.dll	1 ⌄
_hashlib.pyd	1 ⌄
_asyncio.pyd	1 ⌄
QtOpenGLWidgets.pyd	1 ⌄
QtSpatialAudio.pyd	1 ⌄
perfmondata.dll	1 ⌄
QtQuickWidgets.pyd	1 ⌄
QtXml.pyd	1 ⌄
QtWebSockets.pyd	1 ⌄
QtWebEngineWidgets.pyd	1 ⌄
win32file.pyd	1 ⌄
win32console.pyd	1 ⌄

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

_overlapped.pyd	1
_ctypes.pyd	1
win32trace.pyd	1
Qt6SvgWidgets.dll	1
pvectorc.cp39-win_amd64.pyd	1
_queue.pyd	1
Qt6QuickControls2.dll	1
Qt6WebEngineQuickDelegatesQml.dll	1
win32crypt.pyd	1
win32profile.pyd	1
win32lz.pyd	1
win32transaction.pyd	1
_socket.pyd	1
md.cp39-win_amd64.pyd	1
win32ts.pyd	1
Qt6Quick3DSpatialAudio.dll	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

nsProcess.dll	1
select.pyd	1
timer.pyd	1
md__mypyc.cp39-win_amd64.pyd	1
Qt6SerialPort.dll	1
QtMultimediaWidgets.pyd	1
QtSvgWidgets.pyd	1
Qt6MultimediaWidgets.dll	1
win32api.pyd	1
QtWebEngineQuick.pyd	1
_sqlite3.pyd	1
axcontrol.pyd	1
dialog.py	1
contexts.py	1
win32ts_logoff_disconnected.py	1
util.py	5

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

GetTokenInformation.py	1
documents.py	1
win32verstamp.py	1
registry.pys	1
perfmon.py	1
NetValidatePasswordPolicy.py	1
scp.py	1
socket_server.py	1
winxptheme.py	1
codecontainer.py	1
combrowse.py	1
asputil.py	1
cat.py	1
storagecon.py	1
olectl.py	1
build.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

dispatcher.py	1
scriptdispatch.py	1
win32evtlogutil.py	1
excelRTDServer.py	1
error.py	2
exception.py	1
login.py	1
CLSIDToClass.py	1
gencache.py	1
pyscript.py	1
dictionary.py	1
interp.py	1
runproc.py	1
activex.py	1
dynamic.py	1
stackframe.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

test_exceptions.py	1
test_win32profile.py	1
testGIT.py	1
testMarshal.py	1
adb.py	1
register.py	1
selecttlb.py	1
connect.py	3
win32pdhutil.py	1
makegwenum.py	1
makegw.py	1
anki-2.1.66-windows-qt6.exe	188
00000000-00007496.00000002.75101.00401000.00000020.mdmp	7
qtconnectivity_ko.qm	1
ddeserver.py	1
ddeclient.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

regpy.py	1
iebutton.py	1
ietoolbar.py	1
timer_demo.py	1
pywin32.pth	1
__init__.py	11
browse_for_folder.py	1
objectPicker.py	1
win32gui_dialog.py	1
serviceEvents.py	1
customprint.py	1
simple_auth.py	1
dlgtest.py	1
pipeTestService.py	1
win32rcparser_demo.py	1
cerapi.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

rasutil.py	2
excelAddin.py	1
outlookAddin.py	1
dibdemo.py	1
view.py	1
walk_shell_folders.py	1
pippo_server.py	1
localized_names.py	1
context_menu.py	1
setup.py	1
icon_handler.py	1
empty_volume_cache.py	1
explorer_browser.py	1
eventsFreeThreaded.py	1
eventsApartmentThreaded.py	1
column_provider.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

copy_hook.py	1
pipeTestServiceClient.py	1
regsetup.py	1
pyscript_rexec.py	1
control.py	1
app.py	1
browser.py	1
basictimerapp.py	1
BrandProject.py	1
bulkstamp.py	1
flash.py	1
CallTips.py	1
factory.py	1
gateways.py	1
cmdline.py	1
cmdserver.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

IDLEenvironment.py	1
universal.py	1
coloreditor.py	1
dbgcommands.py	1
config.py	1
FileSecurityTest.py	1
ControlService.py	1
stdin.py	1
win32gui_taskbar.py	1
dbgpyapp.py	1
intpydde.py	1
fontdemo.py	1
toolbar.py	1
threadedgui.py	1
win32gui_devicenotify.py	1
validate_password.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample’s detonation

PCAP

Memory dumps

win32gui_menu.py	1
desktopmanager.py	1
dlgappcore.py	1
dlgappdemo.py	1
DockingBar.py	1
docview.py	1
formatter.py	1
dojobapp.py	1
show_all_jobs.py	1
dump_link.py	1
dyndlg.py	1
errorSemantics.py	1
FormatParagraph.py	1
find.py	1
frame.py	1
window.py	2

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

dbgcon.py	1
test_clipboard.py	1
test_win32api.py	1
mapiutil.py	1
backupEventLog.py	1
GenTestScripts.py	1
sspicon.py	1
mmsystem.py	1
winnetwk.py	1
win32netcon.py	1
afxres.py	1
winperf.py	1
guidemo.py	1
ntsecuritycon.py	1
help.py	1
hierlist.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

daodump.py	1
pywin32_bootstrap.py	1
setup_d.py	1
intpyapp.py	1
ITransferAdviseSink.py	1
killProcName.py	1
create_link.py	1
localserver.py	1
pywintypes.py	1
ifiltercon.py	1
object.py	1
ModuleBrowser.py	1
status.py	1
testPyComTest.py	1
fail.py	1
ocxtest.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

ocxserialtest.py	1
test_odbc.py	1
testMSOfficeEvents.py	1
testArrays.py	1
makepy.py	1
openGLDemo.py	1
progressbar.py	1
pydumper.py	1
rastest.py	1
regedit.py	1
menutest.py	1
IFileOperationProgressSink.py	1
sgrepmdi.py	1
pysynch.py	1
sliderdemo.py	1
testIterators.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample’s detonation

PCAP

Memory dumps

regutil.py	1
test_sspi.py	1
startup.py	1
testAXScript.py	1
testvb.py	1
testDynamic.py	1
testShellItem.py	1
testmakepy.py	1
test_win32crypt.py	1
test_win32timezone.py	1
testMSOffice.py	1
test.pys	1
testClipboard.py	1
testCollections.py	1
testDCOM.py	1
testDictionary.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

testExchange.py	1 ⌄
testExplorer.py	1 ⌄
test_win32print.py	1 ⌄
test_security.py	1 ⌄
test_win32gui.py	1 ⌄
default.cfg	1 ⌄
ideoptions.py	1 ⌄
testGatewayAddresses.py	1 ⌄
win32gui_demo.py	1 ⌄
testAccess.py	1 ⌄
msoffice.py	1 ⌄
webbrowser.py	1 ⌄
win32fileDemo.py	1 ⌄
win32traceutil.py	1 ⌄
folder_view.py	1 ⌄
objdoc.py	1 ⌄

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample’s detonation

PCAP

Memory dumps

win32comport_demo.py	1
win32gui_struct.py	1
nativePipeTestService.py	1
test_pycomtest.py	1
regcheck.py	1
thread.py	1
toolmenu.py	1
demoutils.py	3
pywin32_testutil.py	1
vss.py	1
document.py	2
win2kras.py	1
win32clipboardDemo.py	1
TraceCollector.py	1
createwin.py	1
win32rcparser.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

winout.py	1
mapisend.py	1
testNetscape.py	1
EvtSubscribe_push.py	1
EvtSubscribe_pull.py	1
BackupRead_BackupWrite.py	1
BackupSeek_streamheaders.py	1
helloapp.py	1
editor.py	1
mdi_pychecker.py	1
excel.pys	1
PythonCOMServer.h	1
PyWinTypes.h	1
qtmultimedia_ca.qm	1
anki-2.1.66-windows-qt6	178
testDictionary.vbs	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

qt_help_ja.qm	1 ˅
qtlocation_ru.qm	1 ˅
qtserialport_ko.qm	1 ˅
qtdeclarative_ar.qm	1 ˅
qtdeclarative_nn.qm	1 ˅
qtconnectivity_da.qm	1 ˅
PythonCOM.h	1 ˅
PythonCOMRegister.h	1 ˅
pippo.idl	1 ˅
testxslt.js	1 ˅
test.rc	1 ˅
test.h	1 ˅
Anki.lnk	1 ˅
qtwebsockets_ru.qm	1 ˅
qtwebsockets_ko.qm	1 ˅
qtconnectivity_ca.qm	1 ˅

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample’s detonation

PCAP

Memory dumps

qtdeclarative_hr.qm	1
qtwebengine_ko.qm	1
readme.html	1
test1.asp	1
caps.asp	1
test.asp	1
tag.svg	1
deck.svg	1
heart.svg	1
notetype.svg	1
collection.svg	1
clock.svg	1
card-state.svg	1
form.htm	1
demo_intro.htm	1
demo_menu.htm	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

dbgtest.htm	1
foo2.htm	1
docwrite.htm	1
demo_check.htm	1
variant.html	1
MarqueeText1.htm	1
test1.html	1
test.html	1
GeneratedSupport.html	1
misc.html	1
QuickStartClientCom.html	1
QuickStartServerCom.html	1
package.html	1
PythonCOM.html	1
docindex.html	1
index.html	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

demo.htm	1 ⌄
calc.htm	1 ⌄
mousetrack.htm	1 ⌄
CreateObject.asp	1 ⌄
tut1.asp	1 ⌄
icons.qrc	1 ⌄
Testpys.sct	1 ⌄
check-light.svg	1 ⌄
chevron-down-light.svg	1 ⌄
chevron-up-light.svg	1 ⌄
circle-medium-light.svg	1 ⌄
drag-horizontal-light.svg	1 ⌄
drag-vertical-light.svg	1 ⌄
magnify-light.svg	1 ⌄
menu-down-light.svg	1 ⌄
menu-up-light.svg	1 ⌄

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

minus-thick-light.svg	1
selection-drag-light.svg	1
check-FG_DISABLED-dark.svg	1
chevron-down-FG_DISABLED-dark.svg	1
chevron-up-FG_DISABLED-dark.svg	1
circle-medium-FG_DISABLED-dark.svg	1
drag-horizontal-FG_SUBTLE-light.svg	1
drag-vertical-FG_SUBTLE-light.svg	1
minus-thick-FG_DISABLED-dark.svg	1
check-FG_DISABLED-light.svg	1
chevron-down-FG_DISABLED-light.svg	1
chevron-up-FG_DISABLED-light.svg	1
circle-medium-FG_DISABLED-light.svg	1
drag-horizontal-FG_SUBTLE-dark.svg	1
drag-vertical-FG_SUBTLE-dark.svg	1
minus-thick-FG_DISABLED-light.svg	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

check-dark.svg	1 ⌄
chevron-down-dark.svg	1 ⌄
chevron-up-dark.svg	1 ⌄
circle-medium-dark.svg	1 ⌄
drag-horizontal-dark.svg	1 ⌄
drag-vertical-dark.svg	1 ⌄
magnify-dark.svg	1 ⌄
menu-down-dark.svg	1 ⌄
menu-up-dark.svg	1 ⌄
minus-thick-dark.svg	1 ⌄
selection-drag-dark.svg	1 ⌄
application-braces-outline.svg	1 ⌄
book-clock-outline.svg	1 ⌄
book-cog-outline.svg	1 ⌄
book-outline.svg	1 ⌄
circle.svg	1 ⌄

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

circle-outline.svg	1 ⌄
clock-outline.svg	1 ⌄
flag-variant.svg	1 ⌄
flag-variant-off-outline.svg	1 ⌄
flag-variant-outline.svg	1 ⌄
form-textbox.svg	1 ⌄
heart-outline.svg	1 ⌄
newspaper.svg	1 ⌄
tag-off-outline.svg	1 ⌄
tag-outline.svg	1 ⌄
qtdeclarative_fi.qm	1 ⌄
qt_help_pl.qm	1 ⌄
IDLE.cfg	1 ⌄
qt.conf	1 ⌄
screen_2.png	1 ⌄
qtdeclarative_ja.qm	1 ⌄

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

qt_help_de.qm	1
pywin32_bootstrap.cpython-39.opt-2.pyc	1
adsicon.py	1
qtwebengine_ru.qm	1
qtwebengine_ca.qm	1
readme.txt	1
qt_help_cs.qm	1
qtmultimedia_cs.qm	1
__init__.cpython-39.opt-2.pyc	3
qtmultimedia_de.qm	1
qtserialport_de.qm	1
qtwebsockets_de.qm	1
qtwebengine_de.qm	1
qtconnectivity_de.qm	1
qtlocation_de.qm	1
debugTest.pys	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

viewstate.py	1 ⌄
win32cred_demo.py	1 ⌄
qtlocation_ca.qm	1 ⌄
qtdeclarative_bg.qm	1 ⌄
Qt6Core.lib	1 ⌄
qtserialport_es.qm	1 ⌄
qtdeclarative_es.qm	1 ⌄
qtwebsockets_es.qm	1 ⌄
qtlocation_es.qm	1 ⌄
qtwebengine_es.qm	1 ⌄
qtconnectivity_es.qm	1 ⌄
qt_help_es.qm	1 ⌄
qtmultimedia_es.qm	1 ⌄
qtlocation_hr.qm	1 ⌄
test_localsystem.py	1 ⌄
qtdeclarative_fa.qm	1 ⌄

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

qtmultimedia_fa.qm	1
fetch_url.py	1
regsave_sa.py	1
set_file_owner.py	1
qtlocation_fr.qm	1
qtwebsockets_fr.qm	1
qtdeclarative_fr.qm	1
qtmultimedia_fr.qm	1
qt_help_fr.qm	1
configui.py	3
bindings.py	1
testDates.py	1
query_information.py	1
list.py	1
testStorage.py	1
search.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

testADOEvents.py	1
testWMI.py	1
testpropsys.py	1
test_bits.py	1
IShellLinkDataList.py	1
IActiveDesktop.py	1
testSHFileOperation.py	1
shellexecuteex.py	1
testShellFolder.py	1
test_win32inet.py	1
testPyScriptlet.js	1
qtdeclarative_da.qm	1
BTN_PrevPage.gif	1
qt_help_gl.qm	1
qtlocation_fi.qm	1
sspi.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

qtdeclarative_hu.qm	1
qtconnectivity_hu.qm	1
qt_help_hu.qm	1
qtlocation_hu.qm	1
qtmultimedia_hu.qm	1
qtconnectivity_hr.qm	1
qtconnectivity_bg.qm	1
qtconnectivity_ru.qm	1
media-record.png	1
EditServiceSecurity.py	1
expressions.py	1
testHost4Dbg.py	1
getfilever.py	1
testxslt.py	1
EditSecurity.py	1
explicit_entries.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

test_addtask.py	1
test_addtask_2.py	1
test_addtask_1.py	1
testServers.py	1
trybag.py	1
IUniformResourceLocator.py	1
filterDemo.py	1
testROT.py	1
testPersist.py	1
testStreams.py	1
dump_clipboard.py	1
sa_inherit.py	1
ds_record.py	1
browseProjects.py	1
IdleHistory.py	1
AutoExpand.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

PyParse.py	1
keycodes.py	1
template.py	1
testall.py	2
testShell.py	1
test_win32rcparser.py	1
test.py	1
dump.py	1
debugger.py	1
leakTest.py	1
testHost.py	1
AutoIndent.py	1
PythonTools.py	1
testPippo.py	1
test_pywintypes.py	1
handles.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

win32netdemo.py	1
EvtFormatMessage.py	1
netbios.py	1
debug.py	1
testvbscript_regexp.py	1
ds_test.py	1
test_win32pipe.py	1
testConversionErrors.py	1
test_win32event.py	1
test_win32guistruct.py	1
test_win32net.py	1
test_win32trace.py	1
test_win32wnet.py	1
mmapfile_demo.py	1
regsecurity.py	1
RegCreateKeyTransacted.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

RegRestoreKey.py	1
testwnet.py	1
axsite.py	1
policySemantics.py	1
vssutil.py	1
win32console_demo.py	1
eventLogDemo.py	1
OpenEncryptedFileRaw.py	1
CopyFileEx.py	1
GetSaveFileName.py	1
SystemParametersInfo.py	1
win32clipboard_bitmapdemo.py	1
print_desktop.py	1
security_enums.py	1
setsecurityinfo.py	1
setkernelobjectsecurity.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

setnamedsecurityinfo.py	1
setuserobjectsecurity.py	1
lsaregevent.py	1
set_file_audit.py	1
list_rights.py	1
account_rights.py	1
get_policy_info.py	1
set_policy_info.py	1
lsastore.py	1
win32servicedemo.py	1
hiertest.py	1
splittst.py	1
tlbrowse.py	1
bitmap.py	1
testxslt.xsl	1
inetcon.py	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

screen_3.png	1
qtmultimedia_it.qm	1
qt_help_it.qm	1
qtserialport_ja.qm	1
qtwebsockets_ja.qm	1
qt_sv.qm	1
qtlocation_ko.qm	1
qtmultimedia_ja.qm	1
qtdeclarative_lv.qm	1
qt_help_sl.qm	1
qt_help_bg.qm	1
CLSIDToClass.cpython-39.opt-2.pyc	1
gencache.cpython-39.opt-2.pyc	1
qtconnectivity_nl.qm	1
qtdeclarative_nl.qm	1
qtlocation_nl.qm	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

qtmultimedia_nl.qm	1
qt_help_nl.qm	1
qtdeclarative_ko.qm	1
qtlocation_da.qm	1
qtdeclarative_ca.qm	1
win32pdhquery.py	1
qtlocation_pl.qm	1
qtconnectivity_pl.qm	1
qtserialport_pl.qm	1
qtwebsockets_pl.qm	1
qtdeclarative_pl.qm	1
qtwebengine_pl.qm	1
qtmultimedia_pl.qm	1
qt_help_pt_BR.qm	1
qtlocation_pt_BR.qm	1
qtdeclarative_pt_BR.qm	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

qtconnectivity_pt_BR.qm	1 ⌄
qtmultimedia_pt_BR.qm	1 ⌄
qt_pt_PT.qm	1 ⌄
qtmultimedia_hr.qm	1 ⌄
qtmultimedia_nn.qm	1 ⌄
qtmultimedia_bg.qm	1 ⌄
qtmultimedia_ar.qm	1 ⌄
qtserialport_ru.qm	1 ⌄
qtdeclarative_ru.qm	1 ⌄
qtmultimedia_ru.qm	1 ⌄
testInterp.vbs	1 ⌄
qt_help_sk.qm	1 ⌄
qtmultimedia_sk.qm	1 ⌄
dbi.py	1 ⌄
debugTest.vbs	1 ⌄
CreateFileTransacted_MiniVersion.py	1 ⌄

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample’s detonation

PCAP

Memory dumps

qtlocation_tr.qm	1
qtdeclarative_tr.qm	1
qtconnectivity_tr.qm	1
qtmultimedia_tr.qm	1
qt_help_tr.qm	1
qtwebengine_uk.qm	1
qtserialport_uk.qm	1
qtconnectivity_uk.qm	1
qtdeclarative_uk.qm	1
qtwebsockets_uk.qm	1
qt_help_uk.qm	1
qtlocation_uk.qm	1
qtmultimedia_uk.qm	1
license.txt	1
License.txt	1
qt_help_ar.qm	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

qt_help_da.qm	1
qt_help_hr.qm	1
scriptutils.py	1
winprocess.py	1
qtwebsockets_ca.qm	1
dynamic.cpython-39.opt-2.pyc	1
build.cpython-39.opt-2.pyc	1
qtlocation_bg.qm	1
qtwebengine_zh_CN.qm	1
qtserialport_zh_CN.qm	1
qtlocation_zh_CN.qm	1
qt_help_zh_CN.qm	1
qtconnectivity_zh_CN.qm	1
qtmultimedia_zh_CN.qm	1
qtmultimedia_zh_TW.qm	1
qtdeclarative_zh_TW.qm	1

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample's detonation

PCAP

Memory dumps

qt_help_zh_TW.qm	1
qtdeclarative_sk.qm	1

Extracted files

⬢ No verdict	162

Strict IOCs

Provides the IOCs (hashes, domains and IPs) from the detonation of this sample.

CSV

JSON

MAEC 5.0

STIX 2.1

Broad IOCs

Provides the IOCs (hashes, domains and IPs) from both the detonation of this sample and from the associated intelligence Falcon Intelligence brings to the report.

CSV

JSON

MAEC 5.0

STIX 2.1

Others

Provides all other resources available from sample’s detonation

PCAP

Memory dumps