

+  
New analysis

Reports

TI

Pricing

Contacts

FAQ

Sign In

Recycle Bin

SwiftPayment Receipt\_Protected.iso

File Commands Tools Favorites Options Help

↑ SwiftPayment Receipt\_Protected.iso - ISO 9660 Joliet archive, unpacked size 752,128 bytes

Name	Size	Packed	Type	Modified	CRC32
SwiftPayment Re...	752,128	752,128	Application	8/11/2019 8:24...	

MOVE YOUR MOUSE TO VIEW SCREENSHOTS

←→

ANYRUN

Start

6:47 AM

Malicious activity

Win7 32 bit  
Complete

SwiftPayment Receipt\_Protected.iso

MD5: D78950F87C18713DE8CFC9FC2D617D5E

Start: 13.08.2019, 09:46    Total time: 120 s

evasion

trojan

rat

agenttesla

keylogger

stealer

Indicators:

EXE

Tracker:

Agent Tesla

Keylogger

Remote Access Trojan

Stealer

Trojan

Get sample

IOC

MalConf

Restart

Text report

Graph

ATT&CK

AI Summary

Export

CPU

RAM

Processes

Filter by PID or name

Only important

3876

WinRAR.exe

"C:\Users\admin\Desktop\SwiftPayment Receipt\_Prot...

EXE

1k

442

108

3008

SwiftPayment Receipt\_Protected.exe

PE

498

1

84

3440

SwiftPayment Receipt\_Protected.exe

PE

EXE

agenttesla

1k

75

91

HTTP Requests

1

Connections

4

DNS Requests

2

Threats

4

Filter by PID, name or url

PCAP

NETWORK

FILES

DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
26941 ms	GET   200: OK	?	3440	SwiftPayment Receipt_Protected.exe		http://checkip.amazonaws.com/	

Warning

[3440] SwiftPayment Receipt\_Protected.exe

Checks for external IP

Try community version for free!

Register now