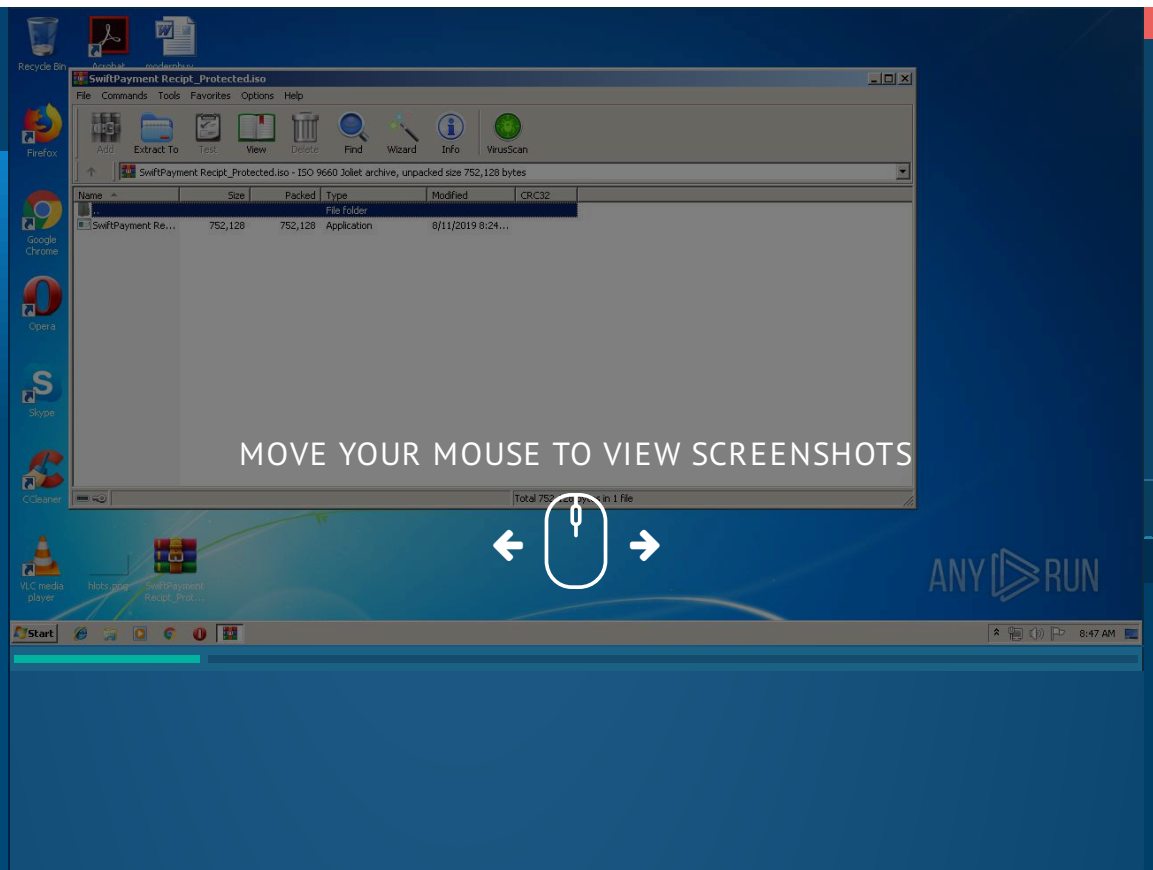

Malicious activity

SwiftPayment Recipt_Protected.iso

MD5: D78950F87C18713DE8CFC9FC2D617D5E

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

Win7 32 bit Complete

evasion trojan rat agenttesla keylogger stealer

Indicators:

Tracker: Agent Tesla, Keylogger, Remote Access Trojan, Stealer, Trojan

Get sample | IOC | MalConf | Restart

Text report | Graph | ATT&CK | AI Summary beta | Export

CPU RAM

Processes Filter by PID or name Only important

3876 WinRAR.exe "C:\Users\admin\Desktop\SwiftPayment Recipt_Prot... 1k 442 108

3008 SwiftPayment Recipt_Protected.exe PE 498 1 84

3440 SwiftPayment Recipt_Protected.exe PE 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 Recipt_Protected.exe		http://checkip.amazonaws.com/	

Warning [3440] SwiftPayment Recipt_Protected.exe Checks for external IP

Try community version for free! Register now