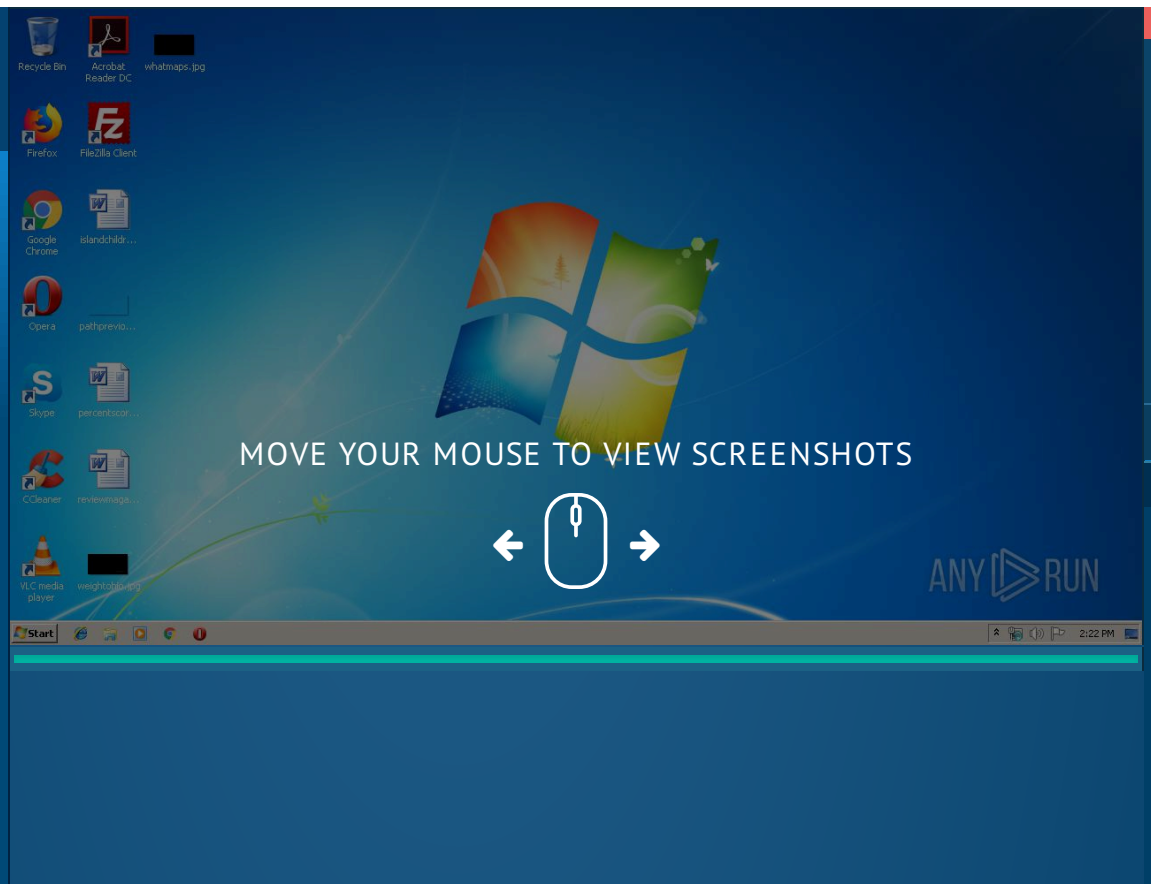

Malicious activity

64uc1

MD5: 6EFD45B1FDDE7E292FC089B8038685E3

Start: 01.10.2019, 15:21 Total time: 300 s

Win7 32 bit Complete

emotet trojan

Indicators: Tracker: Emotet, 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

3468	64uc1.exe	PE				
				232	0	64
976	64uc1.exe	PE	--977a3569			
			emotet	406	45	84
3580	msptermsizes.exe	PE				
				174	0	62
2452	msptermsizes.exe	PE	--f91b2738			
			emotet	494	30	112
2696	o0ZysJD.exe	PE				
				150	0	62
3632	o0ZysJD.exe	PE	--975bd459			
			emotet	408	24	86
4056	msptermsizes.exe	PE				
				174	0	62
2728	msptermsizes.exe	PE	--f91b2738			
			emotet	312	18	

HTTP Requests 2 | Connections 2 | DNS Requests 0 | Threats 8 | Filter by PID, name or url | PCAP

NETWORK | FILES | DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
20957 ms	POST | 200: OK	?	2452	msptermsizes.exe		http://80.240.141.141:7080/merge/win...	46 82
48601 ms	POST | 200: OK	?	2728	msptermsizes.exe		http://80.240.141.141:7080/report/task...	49 14

Danger [2728] msptermsizes.exe Connects to CnC server

Try community version for free! Register now