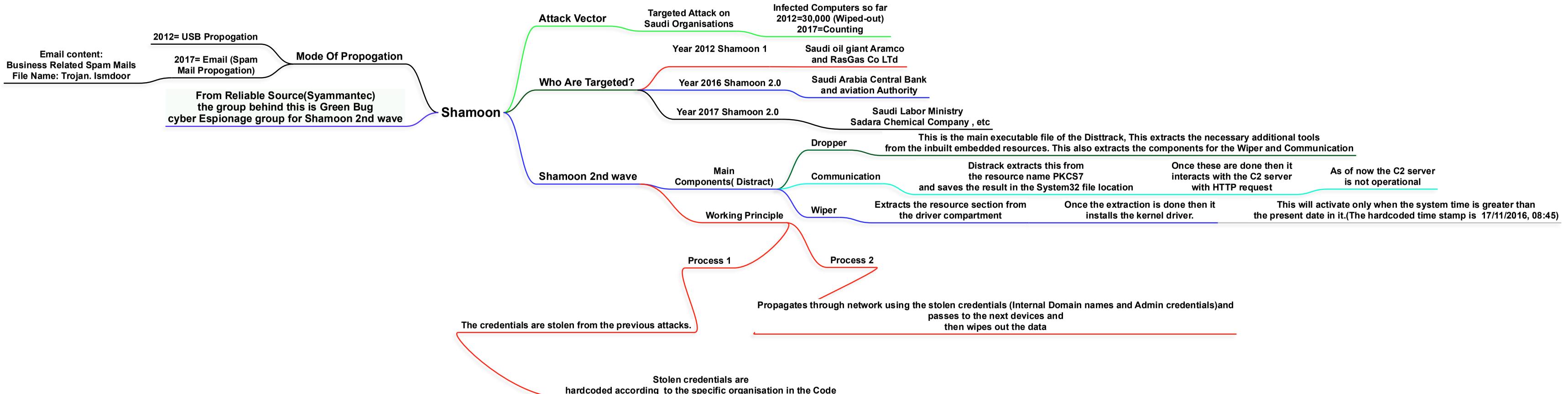
Shamoon
Mode Of Propogation
2012= USB Propogation
2017= Email (Spam Mail Propogation)
Email content: Business Related Spam Mails File Name: Trojan. Ismdoor
From Reliable Source(Syammantec) the group behind this is Green Bug cyber Espionage group for Shamoon 2nd wave
Attack Vector
Targeted Attack on Saudi Organisations
Infected Computers so far 2012=30,000 (Wiped-out) 2017=Counting
Who Are Targeted?
Year 2012 Shamoon 1
Saudi oil giant Aramco and RasGas Co LTd
Year 2016 Shamoon 2.0
Saudi Arabia Central Bank and aviation Authority
Year 2017 Shamoon 2.0
Saudi Labor Ministry Sadara Chemical Company , etc
Shamoon 2nd wave
Main Components(Distract)
Dropper
This is the main executable file of the Disttrack, This extracts the necessary additional tools from the inbuilt embedded resources. This also extracts the components for the Wiper and Communication
Communication
Distrack extracts this from the resource name PKCS7 and saves the result in the System32 file location
Once these are done then it interacts with the C2 server with HTTP request
As of now the C2 server is not operational
Wiper
Extracts the resource section from the driver compartment
Once the extraction is done then it installs the kernel driver.
This will activate only when the system time is greater than the present date in it.(The hardcoded time stamp is 17/11/2016, 08:45)
Working Principle
Process 1
The credentials are stolen from the previous attacks.
Stolen credentials are hardcoded according to the specific organisation in the Code
Process 2
Propagates through network using the stolen credentials (Internal Domain names and Admin credentials)and passes to the next devices and then wipes out the data