|  |  |
| --- | --- |
| HUNT 1:HUNT MAMABEAR | |
| INITIAL ACCESS | VECTOR-PAYLOAD |
| ENUMERATION |  |
| LATERAL MOVEMENT |  |
| PRIVILEGE ESCALATION |  |
| PERSISTENCIE |  |

|  |  |
| --- | --- |
| HUNT 2:HUNT FOR .NET MALWARE IN MEMORY | |
| MEMORY DUMP |  |
|  |  |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
| HUNT 3:HUNT FOR SPECIFIC TTPS | |
| Timestomping MACE attributes (T1099) (timeline between 01/04/2019 and 15/05/2019) |  |
| Meterpreter Migrate command from untrusted process to a trusted one (explorer.exe) (T1055) |  |
| Process Creation through WMI (T1021) (timeline between 01/04/2019 and 01/05/2019) |  |
| MSSQL xp\_cmdshell execution |  |
| Harvesting browser saved credentials (Google Chrome) (T1081) |  |
| Privilege escalation through RottenPotato (T1134) (at 26.05.2019) |  |