Report Codice Malevolo

line 1: 1st Given Name Surname   
line 2: *dept. name of organization*   
*(of Affiliation)*  
 *line 3: name of organization*   
*(of Affiliation)*  
line 4: City, Country  
 line 5: email address or ORCID

I. MALWARE

## *Analisi statica di base*

In questa sezione dovete riportare i risultati dell’analisi statica del PE del malware utilizzando tool quali PEstudio, ExeInfoPE or PEID. In particolare dovete rispondere alle seguenti domande:

* *Il malware e’ impacchettato? Se si quale packer e’ stato utilizzato? Quali sono gli elementi del PE file che indicano che il malware e’ impacchettato?*
* *Quali API vengono importate dal malware? Qual’e’ un possibile comportamento del malware in base alle API importate?*
* *Quali stringhe sono contenute nel malware? Ci sono stringhe che possono che corrispondono a file o cartelle? Oppure sottochiavi del Windows registry? Oppure URL? oppure indirizzi IP?*
* *Alcune delle stringhe sono offuscate o cifrate? Quale codifica o algoritmo di cifratura viene utilizzato?*

## *Analisi dinamica di base*

In questa sezione dovete riportare i risultati dell’analisi dinamica del malware utilizzando tools quali Regshot, e ProcMon. In particolare dovete rispondere alle seguenti domande:

* *Il malware crea o modifica chiavi o sottochiavi del Windows registry? Se si quali ?*
* *Il malware crea o cancella cartelle o file sulla macchina virtuale? Se si quali?*
* *Il malware crea qualche altro processo?*
* *Il malware e’ persistente sulla macchina virtuale? Se si, quale tecnica utilizza per raggiungere persistenza?*

## *Analisi del traffico di rete*

In questa sezione dovete riportare i risultati dell’analisi del traffico di rete con Wireshark e Inetsim. In particolare, dovete rispondere alle seguenti domande:

* *Il malware inizia connessioni di rete? Se si che tipo di traffico genera? Quali URL or indirizzi IP tenta di contattare?*

## *Reverse engineering della funzione indicata*

In questa sezione dovete spiegare il comportamento della funzione assegnata determinato facendo il reverse engineering del codice con IDA, Ghidra e x32dbg.

# IL DOCUMENTO MALEVOLO

## *A.* *Analisi statica*

In questa sezione dovete spiegare i risultati dell’analisi effettuata con strings, exiftool, e yara Poi presentare i risultati ottenuti con i tool di analisi specifici per la tipologi di documento. Per esempio ,se il documento è un pdf riportare i risultati ottenuti con pdfid, pdf-parser e peepdf.

## *B.* *Analisi del codice malevolo contenuto nel documento*

In questa sezione dovete spiegare il comportamento dell’eventuale codice malevolo contenuto all’interno del documento.