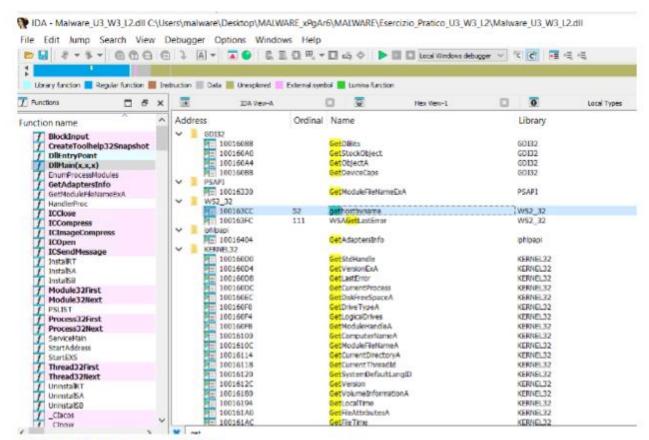


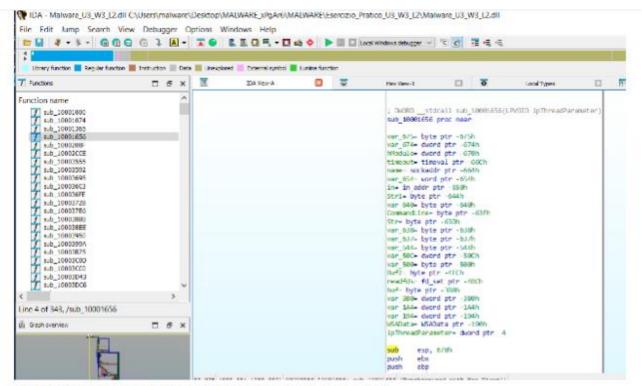
Indirizzo DIIMain -> 10000D02E



indirizzo gethostbyname -> 100163CC

3.

function name	Segment	Start	Length	Locals	Arguments	R	F
f sub_10001000	.text	10001000	00000074	00000110		R	
f sub_10001074	.text	10001074	000002F1	00000064	00000004	R	
f sub_10001365	.text	10001365	000002F1	00000064	00000004	R	
f sub_10001656	.text	10001656	00000A39	00000688	00000004	R	
f sub_1000208F	.text	1000268F	00000C3F	00001B1C	00000018	R	
/ sub_10002CCE	.text	10002CCE	00000887	000015C8	00000018	R	
/ sub_10003555	.text	10003555	0000003D	0000000C		R	
f sub_10003592	.text	10003592	00000103	00000430	00000005	R	
f sub_10003695	.text	10003695	0000002E	00000098		R	
f sub_100036C3	.text	100036C3	00000038	00000098		R	



Ida riconosce in automatico le variabili locali (es var_675 var_674 ecc)
In questo caso sono 24

4.

Non ci sono parametri

Solitamente, i parametri passati via stack vengono referenziati tramite offset da EBP o EBP, come [EBP+8] o [

subito dopo il prologo della funzione.

Non vediamo nessuna di queste istruzioni qui.

5.

All'interno del codice, IDA referenzia alcune stringhe che vengono utilizzate durante l'esecuzione, alcune di esse sono "http://" e "ftp://". Questi due elementi ci portano a pensare che il malware potrebbe utilizzare

una connessione http o ftp, visto che tra gli import vediamo anche la funzione "gethostbyname". Pertanto gli indirizzi che cerca di utilizzare

probabilmente servono per scaricare altre parti del malware mentre la connessione ftp potrebbe servire per esfiltrare dati sensibili sottratti al pc infetto.