REPORT ANALISI MALWARE

FRANCESCO PERSICHETTI

Analizzando il codice del Malware possiamo identificare le librerie che sono state importate:

- KERNEL32.DLL = Libreria piuttosto comune che contiene le funzioni principali per interagire con il sistema operativo, come ad esempio gestione di memoria e manipolazione dei file
- ADVAPI32.DLL = libreria che contiene le funzioni per interagire con i servizi e i registri del sistema operativo Microsoft
- MSVCRT.DLL = libreria che contiene per manipolazione stringhe, allocazione di memoria e altro come chiamate input/output in stile linguaggio C
- WININET.DLL = libreria che contiene funzioni per l'implementazione di alcuni protocolli di rete, come HTTP, FTP, NTP

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

Le sezioni da cui è composto questo Malware sono 3:

- UPX0 = che comprende le istruzioni, ossia le righe di codice che la CPU eseguirà una volta che il software sarà avviato
- UPX1 = contiene dati e variabili globali del programma eseguibile
- UPX2 = contiene informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
00000200	00000208	0000020C	00000210	00000214	00000218	0000021C	00000220	00000222	00000224
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E0000040
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000	C0000040

Ipotizzando il meccanismo di questo malware, si pensa che esso possa raccogliere tutti i dati della vittima per poi inviarli via email all'attaccante