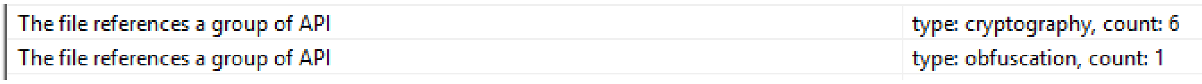
Name - Dnyaneya Dhanwate
Roll No - MT20ACS508
Threat Intelligence

Malware - 2019-06-Nanocore

File Type - .exe [Win32 Executable]
File Size - 1057792 (bytes)
SHA256 - 8274313B5B1E941A67B54E9F311094F2F56A3AFE97820AD03560D9885A60B71B

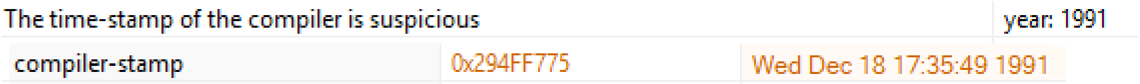
Signature - BobSoft Mini Delphi -> BoB / BobSoft : BobSoft is a packer written in Delphi. BobSoft is commnly used packer for malware to avoid analysis of malware. It means the malware was packed by “BobSoft Mini Delphi”

Entropy: 7.065 : High Entropy value tells us the malware is either encrypted or packed.



The file references a group of API	type: cryptography, count: 6
The file references a group of API	type: obfuscation, count: 1

The above indicators also show obfuscation and cryptography.



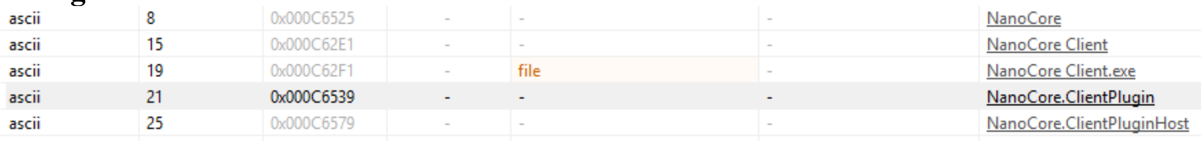
The time-stamp of the compiler is suspicious		year: 1991
compiler-stamp	0x294FF775	Wed Dec 18 17:35:49 1991

The time stamp of compilation has to be fake as the malware surfaced around 2019.

The malware references a URL : 8.0.0.0 which is also suspicious.

The malware is flagged malicious by 61/70 AVs on Virus total.

Strings :



ascii	8	0x000C6525	-	-	-	NanoCore
ascii	15	0x000C62E1	-	-	-	NanoCore Client
ascii	19	0x000C62F1	-	file	-	NanoCore Client.exe
ascii	21	0x000C6539	-	-	-	NanoCore.ClientPlugin
ascii	25	0x000C6579	-	-	-	NanoCore.ClientPluginHost

Above strings are clearly suspicious.

Working of the Malware :
The Malware upon execution it writes the payload in %Temp% folder. The RAT is then loaded into memory by the BobSoft Packer. This then executes the real malware. It also creates a XML file with it’s configuration and it spawns a process that re spawns itself to keep the attack persistent.
These processes then creates TCP connection to it’s command and control and gives control to Author. The malware is a Remote Administrator Tool which gives administrative control to attacker