General Information

SHA 256 HASH	3279fb36cf70bdc4d5ccf02e6be855681a39602a9506fbf4cee0bc92323e6a9d
Architecture	**32 bit binary**
Strings	

Malicious API's

Name	Tags	Malicious
LoadLibraryA	LoadLibraryA is used to load a specified module into the address space of the calling process. Malware commonly use this to load DLLs dynamically for evasion purposes.	Injection Evasion
GetProcAddress	GetProcAddress is used to get the memory address of a function in a DLL. This is often used by malware for obfuscation and evasion purposes to avoid having to call the function directly.	Injection Evasion
VirtualProtect	VirtualProtect is often used by malware to modify memory protection (often to allow write or execution).	Injection

Other API's

FreeSid, ExitProcess, WSARecv, WSAGetLastError

Sections

Name	Virtual Size	Raw Data Size	Virtual Size > Raw Data
UPX0	0xc000	0x0	True
UPX1	0xb000	0xae00	True
.rsrc	0x1000	0xa00	False

Virus Total Results

Magic Header	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Times Submitted	2
Packer PEiD	UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser
Threat Classification sugested label	trojan.swrort/rozenaa
Yara Rules	
Msfpayloads_msf_10	https://github.com/Neo23x0/signature-base