## General Information

| | |
|---|---|
| **SHA 256 HASH** | **3b4773db51a514ef19515b0323fb46691176be163f2a6a71c643f65d9a211867** |
| **Architecture** | **32 bit binary** |
| **Strings** | |

---

## Malicious API's

| Name | Tags | Malicious |
|---|---|---|
| PeekNamedPipe | Used to copy data from a named pipe without removing data from the pipe. This function has been used by exploits targeting SMB vulnerabilities. | Helper |
| ReadFile | ReadFile is used to read data from the specified file or input/output (I/O) device. | Enumeration |
| WriteFile | WriteFile is used to write data to the specified file or input/output (I/O) device. | Helper |
| 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 |
| GetVersionExA | GetVersionExA is a classic method used to retrieve the Windows version. | Enumeration |
| TerminateProcess | TerminateProcess is used to terminate a process. | Helper |
| CreateMutexA | CreateMutexA is used to create a new mutex object. Mutexs are often used by malware to prevent the reinfection of a system with the same or different malware variant. | Helper |
| GetCurrentProcess | GetCurrentProcess is used to retrieve a handle for the current process. | Enumeration |
| GetSystemTimeAsFileTime | Retrieves the current system date and time. The information is in Coordinated Universal Time (UTC) format. This function is commonly used by malware for anti-debugging. | Enumeration Anti-Debugging |
| Sleep | Sleep is used to suspend the execution of the current thread for a set time. This function is commonly used for time-based evasion by adding delays in the code. | Evasion Anti-Debugging |
| WaitForSingleObject | WaitForSingleObject is used to delay the execution of an object. This function is commonly used to allow time for shellcode being executed within a thread to run. It is also used for time-based evasion. | Injection Evasion |
| CreateFileA | CreateFileA is used to create a new file or opens an existing file. | Helper |
| DeviceIoControl | DeviceIoControl is used to send a control message from user space to a device driver. DeviceIoControl is popular with kernel malware because it is an easy flexible way to pass information between user space and kernel space. | Helper |
| connect | Connect is used to establish a connection to a specified socket. | Internet |
| gethostbyname | gethostbyname is used to retrieve host information corresponding to a host name from a host database. | Internet |
| socket | socket is used create a socket that is bound to a specific transport service provider. | Internet |
| closesocket | Closesocket is used to close an existing socket. | Internet |
| select | Select is used to determine the status of one or more sockets waiting if necessary to perform synchronous I/O. This function is used by malware for time-based evasion by setting a large timeout number. | Evasion |
| ioctlsocket | ioctlsocket takes control of the I/O mode of a socket in any state | Internet |
| WSAStartup | WSAStartup is used to initiate use of the Winsock DLL by a process. | Internet |
| WSACleanup | WSACleanup is used to terminate the use of the Winsock 2 DLL. This function is commonly used by malware upon successfully utilizing the Winsock 2 functions. | Internet |

---

## Other API's

strrchr, wcsncmp, wcslen, wcscpy, strerror, modf, strspn, realloc, free, strncmp, strstr, strncpy, qsort, fopen, perror, fclose, fflush, calloc, malloc, signal, printf, atoi, exit, strchr, fprintf, GetExitCodeProcess, LeaveCriticalSection, SetEvent, ReleaseMutex, EnterCriticalSection, DeleteCriticalSection, InitializeCriticalSection, GetFileType, SetLastError, FreeEnvironmentStringsW, GetEnvironmentStringsW, GlobalFree, GetCommandLineW, TlsAlloc, TlsFree, DuplicateHandle, SetHandleInformation, CloseHandle, FileTimeToSystemTime, GetTimeZoneInformation, FileTimeToLocalFileTime, SystemTimeToFileTime, SystemTimeToTzSpecificLocalTime, FormatMessageA, GetLastError, CreateEventA, SetStdHandle, SetFilePointer, CreateFileW, GetOverlappedResult, GetFileInformationByHandle, LocalFree, FreeSid, AllocateAndInitializeSid, getsockopt, htons, ntohl, inet_ntoa, setsockopt, WSAGetLastError, WSARecv, WSASend

---

## Sections

| Name | Virtual Size | Raw Data Size | Virtual Size > Raw Data |
|---|---|---|---|
| .text | 0xa966 | 0xb000 | False |
| .rdata | 0xfe6 | 0x1000 | True |
| .data | 0x705c | 0x4000 | True |
| .rsrc | 0x7c8 | 0x1000 | True |

---

## Virus Total Results

| | |
|---|---|
| **Magic Header** | PE32 executable for MS Windows (GUI) Intel 80386 32-bit |
| **Times Submitted** | 4 |
| **Threat Classification sugested label** | trojan.swrort/cryptz |
| **Yara Rules** | |
| **Msfpayloads_msf_10** | https://github.com/Neo23x0/signature-base |