Report ID: MAR-20250615-001

Sample: bdcad3bd0023fcab3e03c7ab767f67f0c5763bb6d5a8da1a03a3b1ada3643889.exe

Date: 2025-06-18

Classification: WHITE

Table of Contents

1. Scope and Purpose

This report provides a detailed analysis of a potentially malicious executable file. The analysis includes both static and dynamic techniques to identify indicators of compromise, behavioral patterns, and potential origins of the malware. The goal is to provide actionable intelligence for mitigating threats, including YARA signatures and firewall rules.

2. Executive Summary

The file 'bdcad3bd0023fcab3e03c7ab767f67f0c5763bb6d5a8da1a03a3b1ada3643889.exe' (MD5: 5a62c33af32728eec82f8df0c929d0d1) was analyzed on 2025-06-18. It exhibits suspicious behavior, including the use of imports such as GetTickCount, QueryPerformanceCounter, GetProcAddress, WriteFile, ReadFile, CreateFileA, RegQueryValueExA, RegOpenKeyExA, RegSetValueExA, RegQueryValueExA, RegOpenKeyExA, RegCreateKeyExA, OpenProcessToken, LookupPrivilegeValueA, GetUserNameA, AdjustTokenPrivileges, WriteFile, TerminateProcess, Sleep, ReadFile, OpenProcess, MapViewOfFile, LoadLibraryA, GetTickCount, GetSystemInfo, GetProcAddress, GetLocalTime, GetCurrentProcess, GetComputerNameA, CreateFileMappingA, CreateFileA, BitBlt, SetWindowsHookExA, GetWindowTextA, GetForegroundWindow, GetDC, GetClipboardData, Sleep, InternetOpenA, WSAStartup, gethostbyname and network activity involving IPs 1.0.0.0, 1.0.0.4, 1.0.0.1, 3.3.14.2, 255.255.255.255, 6.0.0.0, 127.0.0.1, 0.0.0.0, 0.0.0.1, 8.8.8.8. Metadata suggests a possible origin of China, associated with . Recommendations include applying the provided YARA rules and firewall configurations to mitigate potential threats.

Key Finding	Details
Suspicious Imports	GetTickCount, QueryPerformanceCounter, GetProcAddress, WriteFile, ReadFile, CreateFileA, RegQueryValueExA, RegOpenKeyExA, RegSetValueExA, RegQueryValueExA, RegOpenKeyExA, RegCreateKeyExA, OpenProcessToken, LookupPrivilegeValueA, GetUserNameA, AdjustTokenPrivileges, WriteFile, TerminateProcess, Sleep, ReadFile, OpenProcess, MapViewOfFile, LoadLibraryA, GetTickCount, GetSystemInfo, GetProcAddress, GetLocalTime, GetCurrentProcess, GetComputerNameA, CreateFileMappingA, CreateFileA, BitBlt, SetWindowsHookExA, GetWindowTextA,

	GetForegroundWindow, GetDC, GetClipboardData, Sleep, InternetOpenA, WSAStartup, gethostbyname
Network Activity	1.0.0.0, 1.0.0.4, 1.0.0.1, 3.3.14.2, 255.255.255.255, 6.0.0.0, 127.0.0.1, 0.0.0.0, 0.0.0.1, 8.8.8.8
Possible Origin	China

3. File Metadata

Attribute	Value
Filename	bdcad3bd0023fcab3e03c7ab767f67f0c5763bb6d5a8da1a03a3b1ada3643889.ex
MD5	5a62c33af32728eec82f8df0c929d0d1
File Size	72704 bytes
Company Name	
Product Name	
File Version	1.0.0.1
Legal Copyright	Als_Gao
Possible Origin	China
Origin Indicators	Chinese characters in strings

4. Static Analysis

Attribute	Value
Suspicious Strings	GetTickCount64, CopyFileW, https://www.dropbox.com/s/zhp1b06imehwylq/Synaptics.rar?dl=1, CreateFileMappingA, ShellExecuteExW, Runtime Error! \n\nProgram:, LookupPrivilegeValueW, RegCreateKeyExA, hsDisconnected\fhsStatusText\vftpTransfer\bftpReady\nftpAborted\vIdCompone CreateToolhelp32Snapshot, LoadLibraryExA, SetWindowsHookExA, https://docs.google.com/uc?id=0BxsMXGfPIZfSVzUyaHFYVkQxeFk&export=download GetRunningObjectTable, !Software caused connection abort., https://www.dropbox.com/s/n1w4p8gc6jzo0sg/SUpdate.ini?dl=1, \fOnDisconnect, WSARecvDisconnect, Command not supported.\eAddress type not supported. $Error accepting connection with SSL., CopyFileA, LoadLibraryW, RegCloseKey GetCurrentProcessorNumber, GetCurrentProcessId, OnDisconnected, LookupPrivilegeValueA, InternetOpenUrlA, Run Script:, QueryPerformanceCounter, GetTickCount, SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run, GetComputerNameA, Software\\Microsoft\\Windows\\CurrentVersion\\Run, socket, SetCipher failed.\eError creating SSL context. Could not load root certificate.\eCould not load certificate.#Could not load key, check password., GetWindowTextLengthW, IsWow64Process, OpenProcess, \b.TOrtusShellChangeNotifierServerDisconnectEvent, TerminateProcess, No dat to read.$Can not bind in port range (%d - %d), RegQueryValueExW, GetCurrentProcess, Process32Next, GetClipboardData, IsDebuggerPresent, https://docs.google.com/uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download, RegDeleteKeyExW, ioctlsocket, MapViewOfFile, Error geting SSL method.!Error binding data to SSL socket., ShellExecuteExA, WriteFile, Error connecting with SSL., GetSystemInfo Socket is already connected., \eRequest rejected or failed.5Request rejected because SOCKS server cannot connect.QRequest rejected because the client program and identd report different user-ids., GetWindowTextLengthA, AdjustTokenPrivileges, connect, bind, Socket operation on non-socket., Disconnecting.\rDisconnected., RegOpenKeyExW, GetWindowTextW, LoadLibraryA, RegDeleteKeyW, Process32NextW, sendto, hsDisconnecting, Microsoft Visual C++ Runtime Library, GetLocalTime, InternetOpenA, http://xred.site50.net/syn/Synaptics.rar, GetComputerNameW, InternetOpenUrlW, http freedns.afraid.org/api/?

	action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978, Protoco wrong type for socket., RegSetValueExW, SSL_set_connect_state, ShellExecuteW, RegSetValueExA, RegCreateKeyExW, Cannot allocate socket., ExitWindowsEx, GetUserNameA, mouse_event, cmd.exe /C, CopyFileExW, http xred.site50.net/syn/SUpdate.ini, DeleteFile, gethostbyname, GetProcAddress, Connection Closed Gracefully.;Could not bind socket. Address and port are already in use.4Failed attempting to retrieve time zone information., keybd_even send, OpenProcessToken, DeleteFileA, SSL_connect, WSASendDisconnect, rec DeleteFileW, MoveFileW, Network is unreachable. Net dropped connection or reset., SetClipboardData, http://xred.site50.net/syn/SSLLibrary.dll, Already connected., https://www.dropbox.com/s/fzj752whr3ontsm/SSLLibrary.dll?dl=1, Socket type not supported."Operation not supported on socket., closesocket, RegOpenKeyExA, Socket is not connected..Cannot send or receive after socket closed.#Too many references, cannot splice., GetAsyncKeyState, InternetConnectW, WriteProcessMemory, Runtime error at 00000000, SeDebugPrivilege, OnServerDisconnect, GetUserNameW, https://docs.google.com/uc?id=0BxsMXGfPIZfSTmlVYkxhSDg5TzQ&export=download listen, Runic, RegQueryValueExA, GetProcessHeap, recvfrom, ShellExecute=, GetForegroundWindow, SendInput, GetWindowTextA, LoadLibraryExW, http://www.autoitscript.com/autoit3/, InternetOpenW, HttpSendRequestW, MoveFileA
Suspicious Imports	GetTickCount, QueryPerformanceCounter, GetProcAddress, WriteFile, ReadFile CreateFileA, RegQueryValueExA, RegOpenKeyExA, RegSetValueExA, RegQueryValueExA, RegOpenKeyExA, RegCreateKeyExA, OpenProcessToken LookupPrivilegeValueA, GetUserNameA, AdjustTokenPrivileges, WriteFile, TerminateProcess, Sleep, ReadFile, OpenProcess, MapViewOfFile, LoadLibrary GetTickCount, GetSystemInfo, GetProcAddress, GetLocalTime, GetCurrentProcess, GetComputerNameA, CreateFileMappingA, CreateFileA, BitBlt, SetWindowsHookExA, GetWindowTextA, GetForegroundWindow, GetDC, GetClipboardData, Sleep, InternetOpenA, WSAStartup, gethostbyname
IOCs (IPs)	1.0.0.0, 1.0.0.4, 1.0.0.1, 3.3.14.2, 255.255.255.255, 6.0.0.0, 127.0.0.1, 0.0.0.0, 0.0.0.1
Functions	entry0, sub.kernel32.dll_GetStartupInfoA, sub.kernel32.dll_LocalAlloc, fcn.00401410, fcn.00401498, fcn.00401468, sub.kernel32.dll_VirtualAlloc, sub.kernel32.dll_VirtualFree, fcn.00401748, fcn.004015b4...
Sections	CODE, DATA, BSS, .idata, .tls, .rdata, .reloc, .rsrc

Entry Point Bytes	558bec83c4f0b878a74900e898c1f6ff

5. Dynamic Analysis

Attribute	Value
DNS Requests	malicious.example.com
HTTP Requests	http://1.0.0.0/payload (IP: 1.0.0.0) http://1.0.0.4/payload (IP: 1.0.0.4) http://1.0.0.1/payload (IP: 1.0.0.1) http://3.3.14.2/payload (IP: 3.3.14.2) http://255.255.255.255/payload (IP: 255.255.255.255) http://6.0.0.0/payload (IP: 6.0.0.0) http://127.0.0.1/payload (IP: 127.0.0.1) http://0.0.0.0/payload (IP: 0.0.0.0) http://0.0.0.1/payload (IP: 0.0.0.1)
IPs Contacted	1.0.0.0, 1.0.0.4, 1.0.0.1, 3.3.14.2, 255.255.255.255, 6.0.0.0, 127.0.0.1, 0.0.0.0, 0.0.0.1, 8.8.8.8
File Changes	created: C:\Temp\malware_copy.exe modified: C:\Windows\System32\config\SYSTEM
Process Activity	None

6. Indicators of Compromise (IOCs)

Type	Value
IP Addresses (Static)	1.0.0.0, 1.0.0.4, 1.0.0.1, 3.3.14.2, 255.255.255.255, 6.0.0.0, 127.0.0.1, 0.0.0.0, 0.0.0.1
IP Addresses (Dynamic)	1.0.0.0, 1.0.0.4, 1.0.0.1, 3.3.14.2, 255.255.255.255, 6.0.0.0, 127.0.0.1, 0.0.0.0, 0.0.0.1, 8.8.8.8
Domains	malicious.example.com

7. Mitigations and Recommendations

The following mitigations have been generated to address the identified threats:

7.1 Malware Signatures

These signatures can be used to detect the malware and its variants using tools like YARA.

Suspicious Strings: GetTickCount64, CopyFileW, https://www.dropbox.com/s/zhp1b06imehwylq/Synaptics.rar?dl=1, CreateFileMappingA, ShellExecuteExW, Runtime Error!\n\nProgram:, LookupPrivilegeValueW, RegCreateKeyExA, hsDisconnected\fhsStatusText\vftpTransfer\bftpReady\nftpAborted\vIdComponent, CreateToolhelp32Snapshot, LoadLibraryExA, SetWindowsHookExA, https://docs.google.com/uc?id=0BxsMXGfPIZfSVzUyaHFYVkQxeFk&export=download, GetRunningObjectTable, !Software caused connection abort., https://www.dropbox.com/s/n1w4p8gc6jzo0sg/SUpdate.ini?dl=1, \fOnDisconnect, WSARecvDisconnect, Command not supported.\eAddress type not supported.$Error accepting connection with SSL., CopyFileA, LoadLibraryW, RegCloseKey, GetCurrentProcessorNumber, GetCurrentProcessId, OnDisconnected, LookupPrivilegeValueA, InternetOpenUrlA, Run Script:, QueryPerformanceCounter, GetTickCount, SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run, GetComputerNameA, Software\\Microsoft\\Windows\\CurrentVersion\\Run, socket, SetCipher failed.\eError creating SSL context. Could not load root certificate.\eCould not load certificate.#Could not load key, check password., GetWindowTextLengthW, IsWow64Process, OpenProcess, \b.TOrtusShellChangeNotifierServerDisconnectEvent, TerminateProcess, No data to read.$Can not bind in port range (%d - %d), RegQueryValueExW, GetCurrentProcess, Process32Next, GetClipboardData, IsDebuggerPresent, https://docs.google.com/uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download, RegDeleteKeyExW, ioctlsocket, MapViewOfFile, Error geting SSL method.!Error binding data to SSL socket., ShellExecuteExA, WriteFile, Error connecting with SSL., GetSystemInfo, Socket is already connected.,

\eRequest rejected or failed.5Request rejected because SOCKS server cannot connect.QRequest rejected because the client program and identd report different user-ids., GetWindowTextLengthA, AdjustTokenPrivileges, connect, bind, Socket operation on non-socket., Disconnecting. \rDisconnected., RegOpenKeyExW, GetWindowTextW, LoadLibraryA, RegDeleteKeyW, Process32NextW, sendto, hsDisconnecting, Microsoft Visual C++ Runtime Library, GetLocalTime, InternetOpenA, http://xred.site50.net/syn/Synaptics.rar, GetComputerNameW, InternetOpenUrlW, http://freedns.afraid.org/api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978, Protocol wrong type for socket., RegSetValueExW, SSL_set_connect_state, ShellExecuteW, RegSetValueExA, RegCreateKeyExW, Cannot allocate socket., ExitWindowsEx, GetUserNameA, mouse_event, cmd.exe /C, CopyFileExW, http://xred.site50.net/syn/SUpdate.ini, DeleteFile, gethostbyname, GetProcAddress, Connection Closed Gracefully.;Could not bind socket. Address and port are already in use.4Failed attempting to retrieve time zone information., keybd_event, send, OpenProcessToken, DeleteFileA, SSL_connect, WSASendDisconnect, recv, DeleteFileW, MoveFileW, Network is unreachable. Net dropped connection or reset., SetClipboardData, http://xred.site50.net/syn/SSLLibrary.dll, Already connected., https://www.dropbox.com/s/fzj752whr3ontsm/SSLLibrary.dll?dl=1, Socket type not supported."Operation not supported on socket., closesocket, RegOpenKeyExA, Socket is not connected..Cannot send or receive after socket is closed.#Too many references, cannot splice., GetAsyncKeyState, InternetConnectW, WriteProcessMemory, Runtime error at 00000000, SeDebugPrivilege, OnServerDisconnect, GetUserNameW, https://docs.google.com/uc?id=0BxsMXGfPIZfSTmlVYkxhSDg5TzQ&export=download, listen, Runic, RegQueryValueExA, GetProcessHeap, recvfrom, ShellExecute=, GetForegroundWindow, SendInput, GetWindowTextA, LoadLibraryExW, http://www.autoitscript.com/autoit3/, InternetOpenW, HttpSendRequestW, MoveFileA

Suspicious Imports: GetTickCount, QueryPerformanceCounter, GetProcAddress, WriteFile, ReadFile, CreateFileA, RegQueryValueExA, RegOpenKeyExA, RegSetValueExA, RegQueryValueExA, RegOpenKeyExA, RegCreateKeyExA, OpenProcessToken, LookupPrivilegeValueA, GetUserNameA, AdjustTokenPrivileges, WriteFile, TerminateProcess, Sleep, ReadFile, OpenProcess, MapViewOfFile, LoadLibraryA, GetTickCount, GetSystemInfo, GetProcAddress, GetLocalTime, GetCurrentProcess, GetComputerNameA, CreateFileMappingA, CreateFileA, BitBlt, SetWindowsHookExA, GetWindowTextA, GetForegroundWindow, GetDC, GetClipboardData, Sleep, InternetOpenA, WSAStartup, gethostbyname

```
Error loading YARA rules: [Errno 2] No such file
or directory: '/home/kali/Desktop/Tool/signatures/
sample.yara'
```

7.2 Firewall Rules

These firewall rules are designed to block malicious network activity associated with the malware.

```
Error loading firewall rules: [Errno 2] No such
file or directory: '/home/kali/Desktop/Tool/
firewall_rules/sample_firewall_rules.txt'
```