Threat Analysis Report

Summary

Threat Level	Informational
File Name	HxCEdit.exe
MD5 Hash Identifier	F881B758FF3C37B50493C5DC8B21ED25
SHA-1 Hash Identifier	757C779216B0B6B1EE5679D808442DE7CC4AAFDD
SHA-256 Hash Identifier	2F558A847052F281013C4782CC104321EB09FDCA398C83F10EBBE011B7366CF8
File Size	9998848 bytes
File Submitted	2017-02-24 09:19:19
Duration	482 seconds
Sandbox Replication	168 seconds
Screenshots	12

Engine Analysis

Engine	Threat Name	Severity
GTI File Reputation		
Gateway Anti-Malware		
Anti-Malware	---	Unverified
YARA		
Custom Rules		
Sandbox		Low
Final		Low

Sample is somewhat suspicious: final severity level 2

Behavior Classification

Data spying, Sniffing, Keylogging, Ebanking Fraud	Low
Hiding, Camouflage, Stealthiness, Detection and Removal Protection	Unverified
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection	Unverified
Spreading	Unverified
Exploiting, Shellcode	Unverified
Networking	Unverified
Persistence, Installation Boot Survival	Unverified

Dynamic Analysis

Action	Severity
Set hook procedure to control system activities	Low

Processes Analyzed

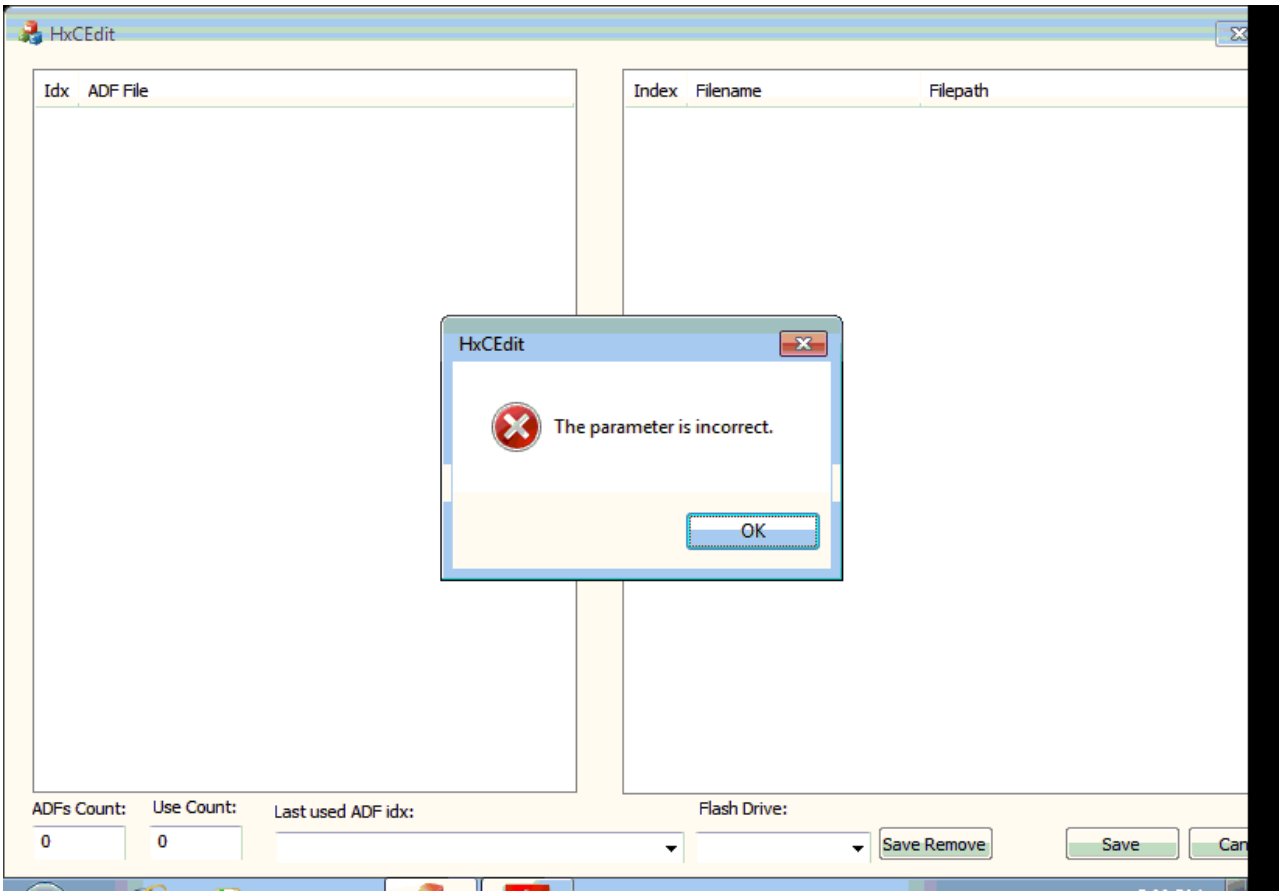
Name	Reason	Severity
HxCEdit.exe	loaded by MATD Analyzer	Low

Screenshots

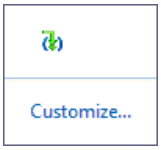
Note: a pop-up window was detected during dynamic analysis so user interaction may be required in order to fully analyze this sample

Images: 12

1056e6.jpg



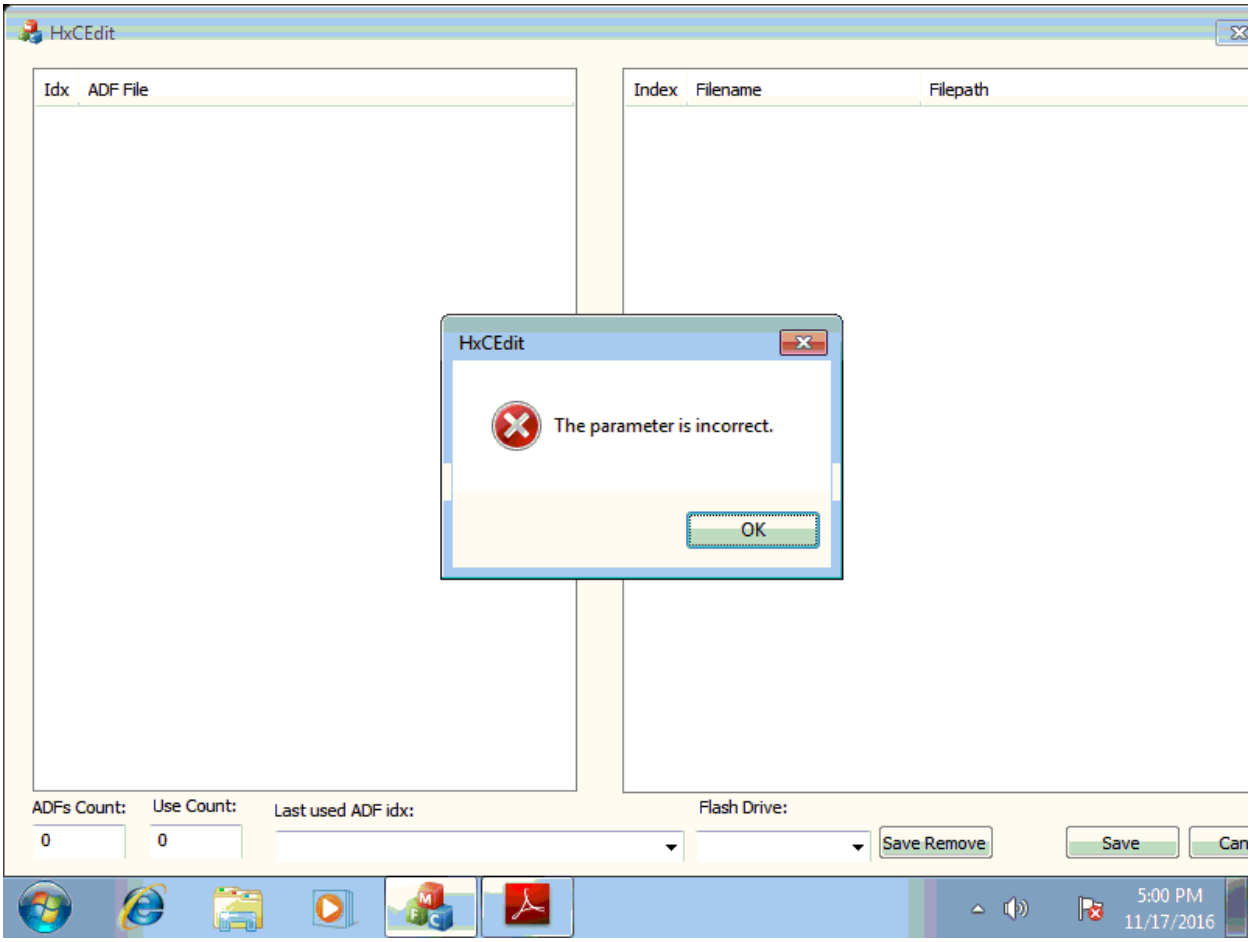
e30c0.jpg



f98a6.jpg



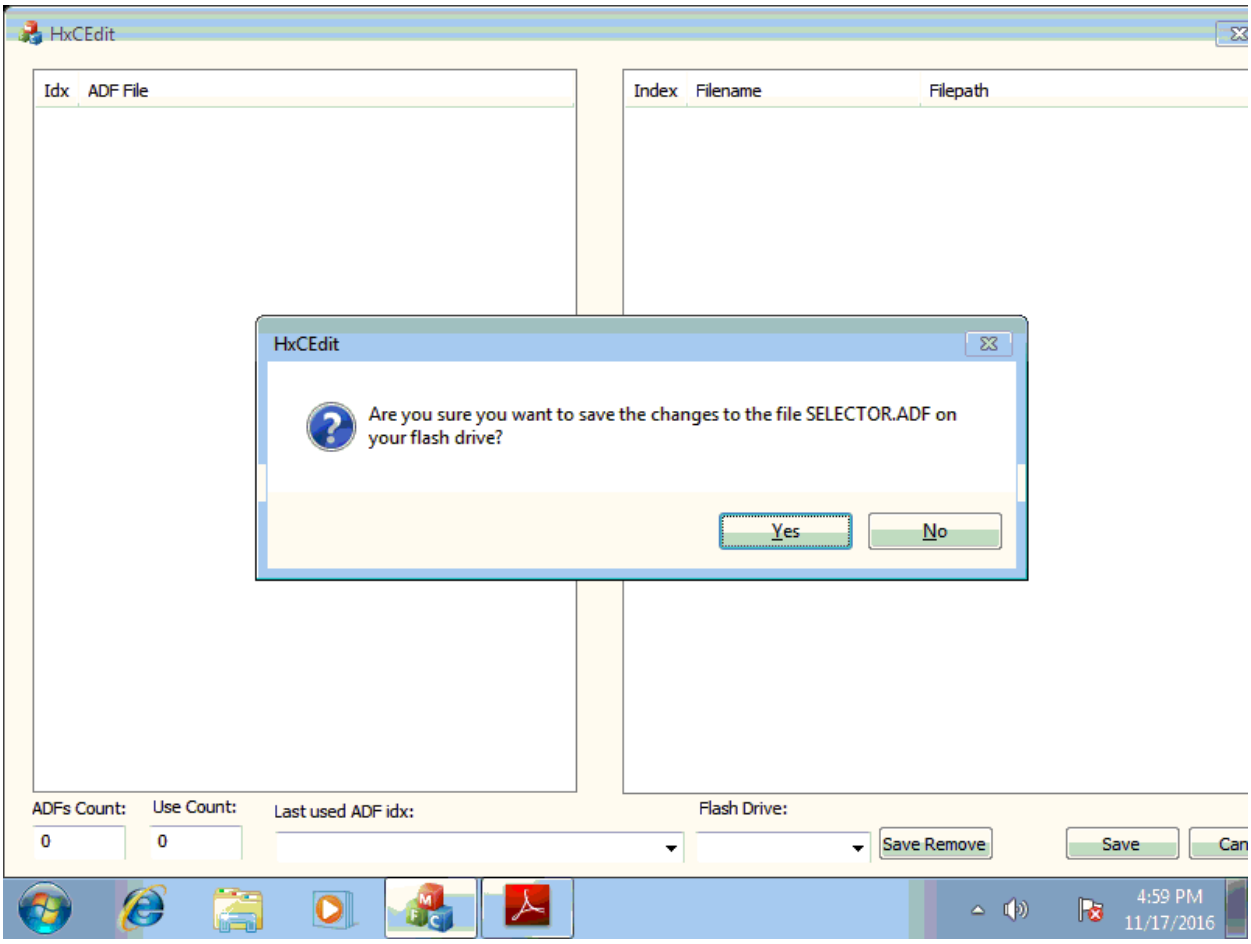
fc88c.jpg



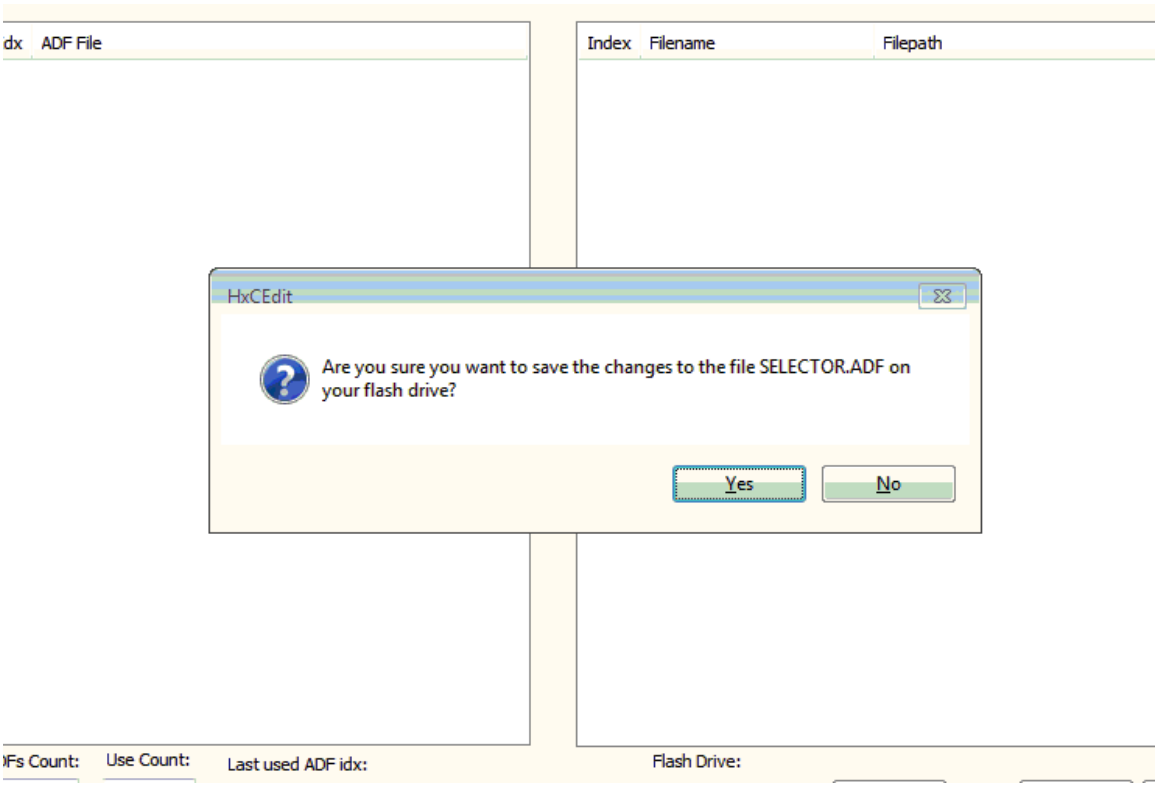
1099ce.jpg



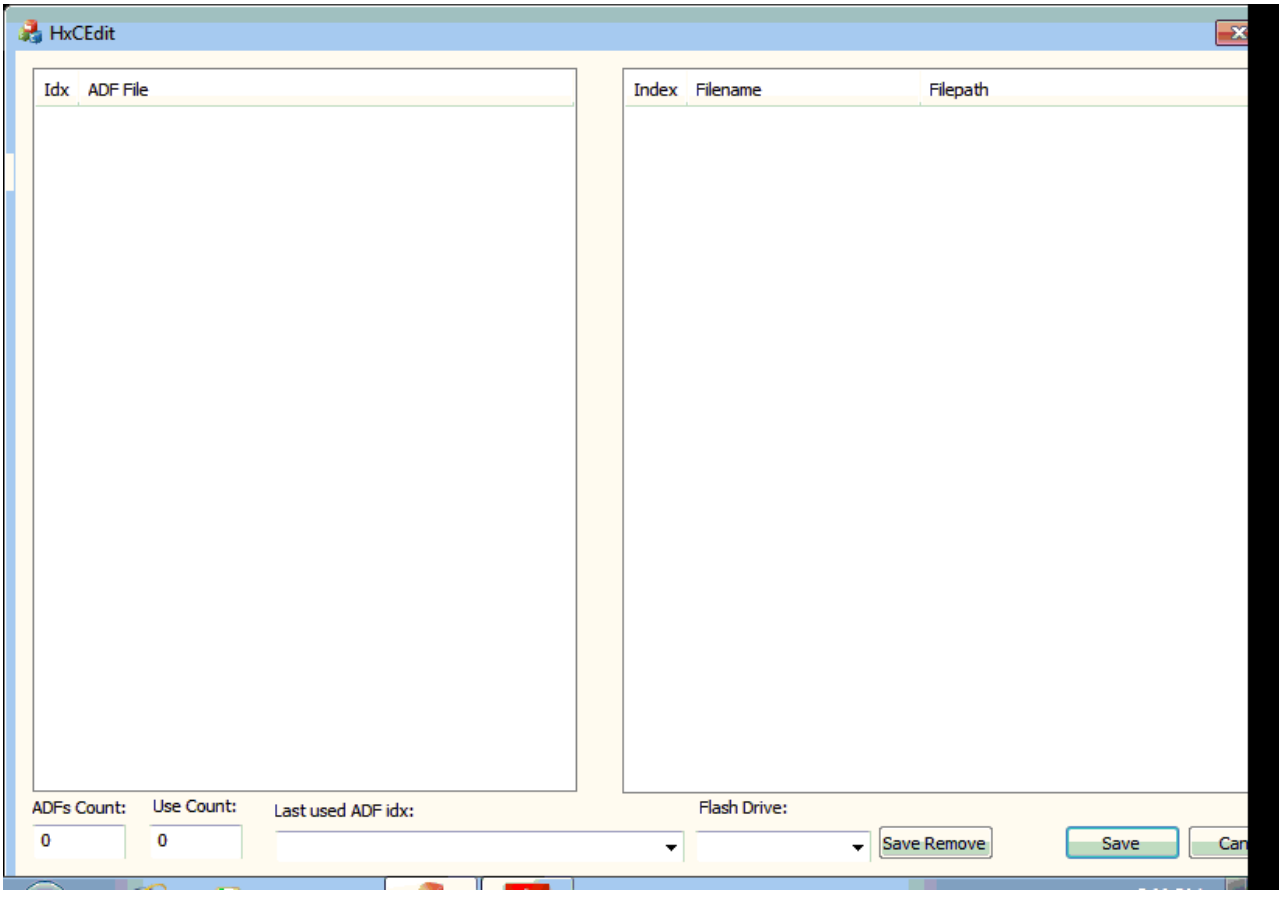
ed806.jpg



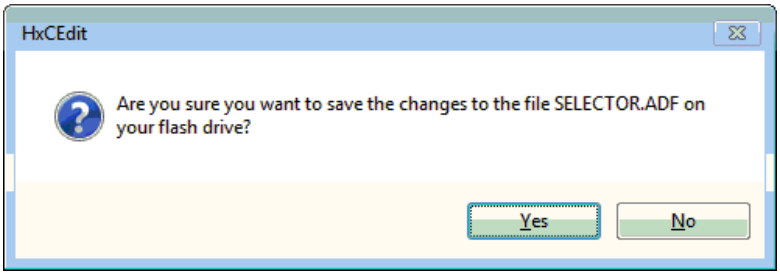
f69ca.jpg



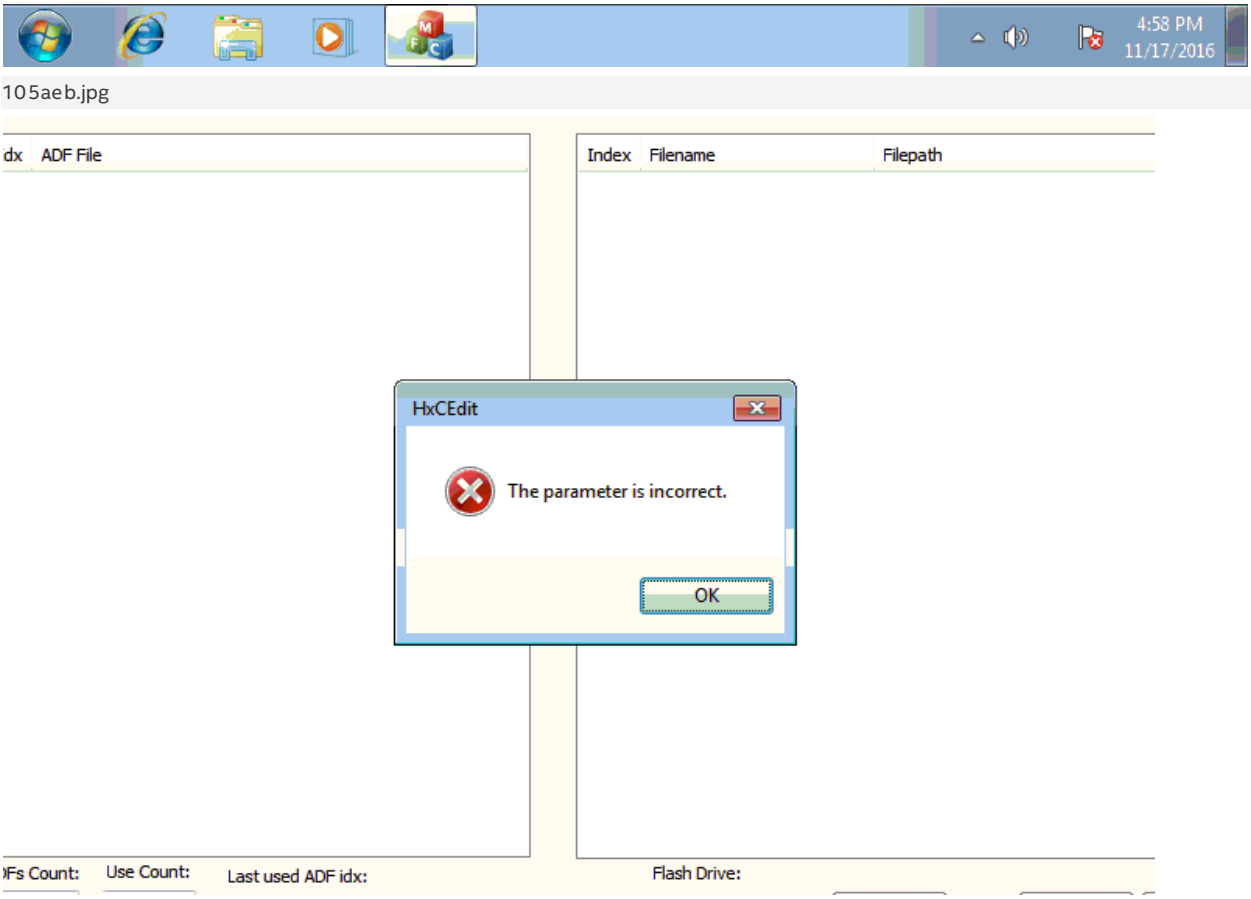
1008e5.jpg



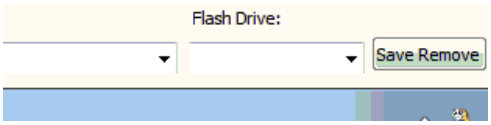
f08c6.jpg



e2c9b.jpg



105aeb.jpg



e0c9d.jpg

HxCEdit.exe

▶ **Run-Time Dlls: 3**

hxceditenu.dll

hxceditloc.dll

comctl32.dll

▶ **File Operations: 4**

Memory Mapped Files

Opened a named file-mapping object

Other

Determined whether a disk drive C:\ is a removable, fixed, CD-ROM, RAM disk, or network drive

Obtained a bitmask representing the currently available disk drives

Retrieved the full path for the module

▶ **Registry Operations: 9**

Registry Opened

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Network

Registry Read

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	**NoClose**
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	**NoDrives**

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoNetConnectDisconnect
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoRecentDocsHistory
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoRun
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	RestrictRun

Process Operations: 8

Other

Deactivated the activation context corresponding to the specified cookie

Enabled an application to supersede the top-level exception handler

Install a new hook procedure (type: WH_CBT)

Install a new hook procedure (type: WH_MSGFILTER)

Obtained the identifier of the thread or process that created the specified window

Opened the access token associated with a thread

Queried the activation context

Retrieved information on a specific string in the current activation context

Network Operations: 1

Socket Activities

Initiated WS2_32 socket DLL

Other Operations: 3

Signal Objects

Mutex-Object Name

Opened an existing named event object

Others

Obtained the system metric or system configuration setting

Retrieved an integer from a key in a section of the Win.ini file

---

File Details

File Type	PE32 executable (GUI) Intel 80386
Digital Signature Verified	Unsigned
Publisher	Not Available
Company	Decision Development derrow@yahoo.com
Description	HxCEdit
Product Name	HxCEdit
Version Info	0.0.0.1
File version	0.0.0.1
MachineType	Decision Development derrow@yahoo.com
Binary Version	0.0.0.1
Strong Name	Not Available
Original Name	HxCEdit.exe
Internal Name	HxCEdit.exe
Copyright	(c) DD derrow@yahoo.com
Comments	Not Available

Analysis Environment

Microsoft Windows 7 Professional Service Pack 1 (build 7601, version 6.1.7601), 64-bit

Internet Explorer version: 8.0.7601.17514

Microsoft Office version: 2003

PDF Reader version: 9.3

No Flash player installed

Flash player plugin version: 14.0.0.179

Platform Version 3.6.2.21.57069

Detection Package Version 3.6.2.21.57069

Baitexe activated but not infected

Copyright © 2016 McAfee, Inc., 2821 Mission College Blvd, Santa Clara, CA 95054, www.intelsecurity.com