WildFire Analysis Report

Table of Contents

1 File Information

File Type	PE
File Signer	
SHA-256	317e196e81c5f73c5eaf026f406cc56efb66c0b170e03885dcc78e5ebc006855
SHA-1	772d629837b3ca3264949ce000b193fedd3822b6
MD5	bd335fb137557dd9b10ebf73e855cb56
File Size	312426 bytes
First Seen Timestamp	2015-08-12 04:01:43 PDT
Verdict	Malware
Antivirus Coverage	VirusTotal Information

2 Dynamic Analysis

2.1. VM1 (Windows XP, Adobe Reader 9.4.0, Flash 10, Office 2007)

2.1.1. Behavioral Summary

This sample was found to be **malware** on this virtual machine.

Behavior	Severity
Sample registered a Graphical User Interface callback Malware can use callbacks exposed by the operating system as a means to instrument the infected system	
Created an executable file in the Windows folder The Windows folder contains the core components of the Windows operating system. Malware often places executables in this folder to avoid detection.	
Created or modified a file in the Windows system folder The Windows system folder contains configuration files and executables that control the underlying functions of the system. Malware often modifies the contents of this folder to manipulate the system, establish persistence, and avoid detection.	
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	
Started a process A process running on the system may start additional processes to perform actions in the background. This behavior is common to legitimate software as well as malware.	
Created a file in the Windows folder The Windows folder contains the core components of the Windows operating system. Malware often modifies the contents of this folder to manipulate the system, establish persistence, and avoid detection.	
Generated unknown TCP or UDP traffic Legitimate software typically uses well-known application protocols to communicate over a network. In some cases, however, legitimate software may use proprietary protocols. Malware commonly uses custom protocols to avoid detection, and a sample that generates unknown TCP or UDP traffic in this way is often malicious.	
Modified the Windows Registry The Windows Registry houses system configuration settings and options, including information about installed applications, services, and drivers. Malware often modifies registry data to establish persistence on the system and avoid detection.	
Modified Portable Executable image sections at runtime Portable Executable images contain sections with different access and execution permissions. These sections are built statically	

during compilation, and runtime modifications indicate binary obfuscation techniques.	
Modified Internet Explorer security settings Modern browsers provide a variety of security controls that are effective at mitigating or preventing malicious activity. Malware often modifies the settings for these controls to subvert a system's built-in security measures.	
Restarted itself in a suspicious manner Malware often exits and restarts itself to avoid detection.	

2.1.2. Network Activity

DNS Queries

Domain Name	Query Type	DNS Response
lozjapo.net	NS	ns1.reg.ru
lozjapo.net	A	78.136.221.159
lozjapo.net	NS	ns2.reg.ru

Connections

Host	Port	Protocol	Country
78.136.221.159	443	TCP	RU

2.1.3. Host Activity

Process Name - "c:\documents and settings\administrator\sample.exe"

(command: "c:\documents and settings\administrator\sample.exe")

No activity recorded for this process.

Process Name - sample.exe

(command: c:\documents and settings\administrator\sample.exe)

Process Activity

Child Process	Action
"c:\documents and settings\administrator\sample.exe"	Create

Event Timeline

1 Created Process c:\documents and settings\administrator\sample.exe
2 Created Process "c:\documents and settings\administrator\sample.exe"

2.2. VM2 (Windows 7 x64 SP1, Adobe Reader 11, Flash 11, Office 2010)

2.2.1. Behavioral Summary

This sample was found to be **malware** on this virtual machine.

Behavior	Severity

Sample registered a Graphical User Interface callback Malware can use callbacks exposed by the operating system as a means to instrument the infected system	
Created an executable file in the Windows folder The Windows folder contains the core components of the Windows operating system. Malware often places executables in this folder to avoid detection.	
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	
Started a process from a user folder User folders are storage locations for music, pictures, downloads, and other user-specific files. Malware often runs executable content out of these folders to avoid detection, while legitimate applications are usually run out of the Windows, Windows system, or Program Files folders.	
Disabled Internet Explorer Phishing Filter Internet Explorer provides a variety of security controls that are effective at mitigating or preventing malicious activity, including a Phishing Filter. Malware often disables the Phishing Filter so that users are not alerted when visiting known malicious websites.	
Started a process A process running on the system may start additional processes to perform actions in the background. This behavior is common to legitimate software as well as malware.	
Generated unknown TCP or UDP traffic Legitimate software typically uses well-known application protocols to communicate over a network. In some cases, however, legitimate software may use proprietary protocols. Malware commonly uses custom protocols to avoid detection, and a sample that generates unknown TCP or UDP traffic in this way is often malicious.	
Used SSL SSL is a certificate-based cryptographic protocol for secure communication over the Internet. Malware often communicates over SSL to hide its traffic from network security systems, like most firewalls and IPSes, that do not offer SSL decryption.	
Modified the Windows Registry to enable auto-start for a file in a user folder The Windows Registry Run keys allow an application to specify that it should be launched during system startup. Malware often leverages this mechanism to ensure that it will be run each time the system boots up, and may run content out of a user folder to avoid detection.	
Modified the Windows Registry to enable auto-start The Windows Registry Run keys allow an application to specify that it should be launched during system startup. Malware often leverages this mechanism to establish persistence on the system and ensure that it will be run each time the system boots up.	
Modified the Windows Registry The Windows Registry houses system configuration settings and options, including information about installed applications, services, and drivers. Malware often modifies registry data to establish persistence on the system and avoid detection.	
Modified Internet Explorer security settings Modern browsers provide a variety of security controls that are effective at mitigating or preventing malicious activity. Malware often modifies the settings for these controls to subvert a system's built-in security measures.	
Injected code into another process The Windows API provides several functions for code injection, including CreateRemoteThread(), WriteProcessMemory(), LoadLibrary(), and SetWindowsHookEx(). While these functions are sometimes called in legitimate applications, most often they are used by malware to execute an attack through a trusted process while avoiding detection.	
Modified connections settings for Internet Explorer Internet Explorer provides a variety of settings for Internet connections, Virtual Private Networks (VPNs), proxies, and Local Area Networks (LANs). Malware often changes these settings to control the flow of traffic to and from the system.	
Attempted to sleep for a long period Malware analysis environments have a limited amount of time in which to execute code and deliver a verdict. To subvert this	

process, malware often delays execution, or "sleeps," for a long period, allowing it to avoid detection.	
Modified Portable Executable image sections at runtime Portable Executable images contain sections with different access and execution permissions. These sections are built statically during compilation, and runtime modifications indicate binary obfuscation techniques.	
Invoked an important system command Malware often creates and injects itself into system processes to evade detection.	
Restarted itself in a suspicious manner Malware often exits and restarts itself to avoid detection.	
Modified proxy settings for Internet Explorer Rather than communicate directly with a server, a client may route requests through a proxy. If the proxy is malicious, it may modify what a user sees when accessing web pages or even execute a man-in-the-middle (MITM) attack, potentially gaining access to sensitive user information.	

2.2.2. Network Activity

DNS Queries

Domain Name	Query Type	DNS Response
time.windows.com	A	104.209.134.106
akadns.net	NS	a7-131.akadns.net
akadns.net	NS	a3-129.akadns.net
lozjapo.net	A	78.136.221.159
akadns.net	NS	a28-129.akadns.org
akadns.net	NS	a9-128.akadns.net
akadns.net	NS	a13-130.akadns.org
lozjapo.net	NS	ns1.reg.ru
akadns.net	NS	a5-130.akadns.org
lozjapo.net	NS	ns2.reg.ru
akadns.net	NS	a4-131.akadns.org
akadns.net	NS	a11-129.akadns.net
akadns.net	NS	a10-128.akadns.org
akadns.net	NS	a1-128.akadns.net

Connections

Host	Port	Protocol	Country
104.209.134.106	123	UDP	N/A
78.136.221.159	443	TCP	RU

2.2.3. Host Activity

Process Name - vssadmin.exe Delete Shadows /All /Quiet

(command: vssadmin.exe Delete Shadows /All /Quiet)

No activity recorded for this process.

Process Name - "C:\Users\Administrator\sample.exe"

(command: "C:\Users\Administrator\sample.exe")

Process Activity

Child Process	Action

C:\Windows\system32\explorer.exe	Create

File Activity

File	Action	Size(B)	File Type	Hash
C:\ProgramData\yvyjivorapadumok\01000000	Create	312432	unknown	md5:ea3830bf2e1aab0ace4164e6972782cb sha1:3da9b2cc0e66230486ba5a758feb8c909366442c sha256:3a6b9a8761eb3f7fbd6ccc28325408e7c591385c7b03241c4be4388e868da968

Created Mutexes

Mutex Name
<NULL>
Global\uzyvejoqubypihubuwanyhy
Global\idetihakydefunijykadogiqadiwoku

Process Name - explorer.exe

(command: C:\Windows\system32\explorer.exe)

Process Activity

Child Process	Action
vssadmin.exe Delete Shadows /All /Quiet	Create

File Activity

File	Action	Size(B)	File Type	Hash
C:\Windows\rkaqoguz.exe	Create	312426	exe	md5:bd335fb137557dd9b10ebf73e855cb56 sha1:772d629837b3ca3264949ce000b193fedd3822b6 sha256:317e196e81c5f73c5eaf026f406cc56efb66c0b170e03885dcc78e5ebc006855
C:\ProgramData\yvyjivorapadumok\02000000	Create	64	unknown	md5:8286ddd0b4628205e72783fbdcedef07 sha1:893f24bb32dcb35281c0cd928c309d10ce1798a5 sha256:aee2f424f70730478e647d851359106089cec9e47450290487d239c391b8d75b

C:\ProgramData\yvyjivorapadumok\00000000	Create	16	unknown	md5:16f403c9603478f028ab251056ad1933 sha1:e5af749948b132f2e4f1e3809a8719554fe8eed5 sha256:94717e0b48e06701a3406155ff61639e5c1f01ef642447723760ac5949776507

Registry Activity

Registry Key	Value	Action
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run		Create
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings		Create
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\PhishingFilter		Create
\REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections		Create
\REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\windows\CurrentVersion\Internet Settings		Create
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109A10090400000000000F01FEC\Usage		Create
\REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages		Create
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles		Create
\REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{30C41AD1-F80F-4713-B56F-B1E1D2CE9DA9}		Create
\REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{30C41AD1-F80F-4713-B56F-B1E1D2CE9DA9}\06-09-e2-fb-19-b9		Create
\REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\06-09-e2-fb-19-b9		Create
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\Schannel		Create
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\alufecom	"C:\Windows\rkaqoguz.exe"	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Internet Explorer\PhishingFilter\EnabledV8	0	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Internet Explorer\PhishingFilter\EnabledV9	0	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable	0	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings	NULL	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109A10090400000000000F01FEC\Usage\OutlookMAPI2Intl_1033	1191968769	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-38943	Off	Set

2370-500\Software\Microsoft\Office\14.0\Common\Language Resources\EnabledLanguages\1033		
\REGISTRY\USER\S-1-5-21-3141258405-581381896-38943 2370-500\Software\Microsoft\Office\14.0\Common\Language Resources\EnabledLanguages\1033	On	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-38943 2370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{30C41AD1-F80F-4713-B56F-B1E1D2CE9DA9}\WpadDecisionReason	1	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-38943 2370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{30C41AD1-F80F-4713-B56F-B1E1D2CE9DA9}\WpadDecisionTime	NULL	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-38943 2370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{30C41AD1-F80F-4713-B56F-B1E1D2CE9DA9}\WpadDecision	3	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-38943 2370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{30C41AD1-F80F-4713-B56F-B1E1D2CE9DA9}\WpadNetworkName	Network 4	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-38943 2370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\06-09-e2-fb-19-b9\WpadDecisionReason	1	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-38943 2370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\06-09-e2-fb-19-b9\WpadDecisionTime	NULL	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-38943 2370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\06-09-e2-fb-19-b9\WpadDecision	3	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-38943 2370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings	NULL	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-38943 2370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork	{30C41AD1-F80F-4713-B56F-B1E1D2CE9DA9}	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-38943 2370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	0	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-38943 2370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	1	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-38943 2370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{30C41AD1-F80F-4713-B56F-B1E1D2CE9DA9}\WpadDecision	0	Set
\REGISTRY\USER\S-1-5-21-3141258405-581381896-38943 2370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\06-09-e2-fb-19-b9\WpadDecision	0	Set

Created Mutexes

Mutex Name
<NULL>
Global\idetihakydefunijykadogiqadiwoku
IESQMMUTEX_0_208
Local\!IETld!Mutex

Process Name - sample.exe

(command: C:\Users\Administrator\sample.exe)

Process Activity

Child Process	Action
"C:\Users\Administrator\sample.exe"	Create

Event Timeline

1 Created Process C:\Users\Administrator\sample.exe
2 Created Process "C:\Users\Administrator\sample.exe"
3 Created mutex
4 Created mutex Global\uzyvejoqubypihubuwanyhy
5 Created mutex Global\idetihakydefunijykadogiqadiwoku
6 Created file C:\ProgramData\yvyjivorapadumok\01000000
7 Created Process C:\Windows\system32\explorer.exe
8 Created mutex
9 Created mutex Global\idetihakydefunijykadogiqadiwoku
10 Created file C:\Windows\rkaqoguz.exe
11 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\alufecom to value "C:\Windows\rkaqoguz.exe"
12 Created file C:\ProgramData\yvyjivorapadumok\02000000
13 Created file C:\ProgramData\yvyjivorapadumok\00000000
14 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Internet Explorer\PhishingFilter\EnabledV8 to value 0
15 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Internet Explorer\PhishingFilter\EnabledV9 to value 0
16 Created Process vssadmin.exe Delete Shadows /All /Quiet
17 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable to value 0
18 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings to value NULL
19 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109A10090400000000000F01FEC\Usage\OutlookMAPI2Intl_1033 to value 1191968769
20 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 to value Off
21 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 to value On
22 Created mutex
23 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{30C41AD1-F80F-4713-B56F-B1E1D2CE9DA9}\WpadDecisionReason to value 1
24 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{30C41AD1-F80F-4713-B56F-B1E1D2CE9DA9}\WpadDecisionTime to value NULL
25 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{30C41AD1-F80F-4713-B56F-B1E1D2CE9DA9}\WpadDecision to value 3
26 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{30C41AD1-F80F-4713-B56F-B1E1D2CE9DA9}\WpadNetworkName to value Network 4
27 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\06-09-e2-fb-19-b9\WpadDecisionReason to value 1
28 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\06-09-e2-fb-19-b9\WpadDecisionTime to value NULL
29 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\06-09-e2-fb-19-b9\WpadDecision to value 3
30 Created mutex IESQMMUTEX_0_208
31 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings to value NULL
32 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork to value {30C41AD1-F80F-4713-B56F-B1E1D2CE9DA9}
33 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet to value 0
34 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect to value 1
35 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet to value 0
36 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect to value 1
37 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet to value 0
38 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect to value 1
39 Created mutex Local\!IETld!Mutex

40 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{30C41AD1-F80F-4713-B56F-B1E1D2CE9DA9}\WpadDecisionReason to value 1
41 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{30C41AD1-F80F-4713-B56F-B1E1D2CE9DA9}\WpadDecisionTime to value NULL
42 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{30C41AD1-F80F-4713-B56F-B1E1D2CE9DA9}\WpadDecision to value 0
43 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{30C41AD1-F80F-4713-B56F-B1E1D2CE9DA9}\WpadNetworkName to value Network 4
44 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\06-09-e2-fb-19-b9\WpadDecisionReason to value 1
45 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\06-09-e2-fb-19-b9\WpadDecisionTime to value NULL
46 Set key \REGISTRY\USER\S-1-5-21-3141258405-581381896-389432370-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\06-09-e2-fb-19-b9\WpadDecision to value 0
47 Created mutex IESQMMUTEX_0_208