Appendix A: Module Logging

Figure 3 displays a sample event message generated by module logging when running the popular `Invoke-Mimikatz` script, with the `-DumpCreds` argument, which is used to steal logon credentials from memory. This is the message body from a single event selected from the larger series of events generated by running the script.

```
ParameterBinding(Out-Default): name="InputObject"; value="Specified cast is not valid."
ParameterBinding(Out-Default): name="InputObject"; value="Specified cast is not valid."
ParameterBinding(Out-Default): name="InputObject"; value="
  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Feb 16 2015 22:15:28)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 15 modules * * */



mimikatz(powershell) # sekurlsa::logonpasswords


Authentication Id : 0 ; 449326 (00000000:0006db2e)
Session           : Interactive from 1
User Name         : me
Domain            : DESKTOP-RMJCHH3
SID               : S-1-5-21-3432306013-2099639235-1280950563-1001
       msv :
        [00000003] Primary
        * Username : me
        * Domain   : DESKTOP-RMJCHH3
        * Flags    : 00/N01/L00/S01/00/00/00/00
        * NTLM     : 89e8c08c50f67f0970f2e5c4adf4ac79
        * SHA1     : defc430d825dc84461199d2b8602d8d23ea279cb
        * unknow   : [0..0]
        [00010000] CredentialKeys
        * NTLM     : 89e8c08c50f67f0970f2e5c4adf4ac79
        * SHA1     : defc430d825dc84461199d2b8602d8d23ea279cb
       tspkg :
       wdigest :
        * Username : me
        * Domain   : DESKTOP-RMJCHH3
        * Password : (null)
       kerberos :
        * Username : me
        * Domain   : DESKTOP-RMJCHH3
        * Password : (null)
       ssp :  KO
       credman :

Authentication Id : 0 ; 449217 (00000000:0006dac1)
Session           : Interactive from 1
User Name         : me
Domain            : DESKTOP-RMJCHH3
```

```
SID               : S-1-5-21-3432306013-2099639235-1280950563-1001
       msv :
        [00010000] CredentialKeys
        * NTLM     : 89e8c08c50f67f0970f2e5c4adf4ac79
        * SHA1     : defc430d825dc84461199d2b8602d8d23ea279cb
        [00000003] Primary
        * Username : me
        * Domain   : DESKTOP-RMJCHH3
        * Flags    : 00/N01/L00/S01/00/00/00/00
        * NTLM     : 89e8c08c50f67f0970f2e5c4adf4ac79
        * SHA1     : defc430d825dc84461199d2b8602d8d23ea279cb
        * unknow   : [0..0]
       tspkg :
       wdigest :
        * Username : me
        * Domain   : DESKTOP-RMJCHH3
        * Password : (null)
       kerberos :
        * Username : me
        * Domain   : DESKTOP-RMJCHH3
        * Password : (null)
       ssp :  KO
       credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
SID               : S-1-5-19
       msv :
       tspkg :
       wdigest :
        * Username : (null)
        * Domain   : (null)
        * Password : (null)
       kerberos :
        * Username : (null)
        * Domain   : (null)
        * Password : (null)
       ssp :  KO
       credman :

Authentication Id : 0 ; 64796 (00000000:0000fd1c)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
SID               : S-1-5-90-0-1
       msv :
       tspkg :
       wdigest :
        * Username : DESKTOP-RMJCHH3$
        * Domain   : WORKGROUP
        * Password : (null)
       kerberos :
       ssp :  KO
       credman :
```

```
Authentication Id : 0 ; 63194 (00000000:0000f6da)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
SID               : S-1-5-90-0-1
       msv :
       tspkg :
       wdigest :
        * Username : DESKTOP-RMJCHH3$
        * Domain   : WORKGROUP
        * Password : (null)
       kerberos :
       ssp :  KO
       credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : DESKTOP-RMJCHH3$
Domain            : WORKGROUP
SID               : S-1-5-20
       msv :
       tspkg :
       wdigest :
        * Username : DESKTOP-RMJCHH3$
        * Domain   : WORKGROUP
        * Password : (null)
       kerberos :
        * Username : desktop-rmjchh3$
        * Domain   : WORKGROUP
        * Password : (null)
       ssp :  KO
       credman :

Authentication Id : 0 ; 41002 (00000000:0000a02a)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
SID               :
       msv :
       tspkg :
       wdigest :
       kerberos :
       ssp :  KO
       credman :

Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : DESKTOP-RMJCHH3$
Domain            : WORKGROUP
SID               : S-1-5-18
       msv :
       tspkg :
       wdigest :
        * Username : DESKTOP-RMJCHH3$
        * Domain   : WORKGROUP
        * Password : (null)
       kerberos :
```

```
        * Username : desktop-rmjchh3$
        * Domain   : WORKGROUP
        * Password : (null)
       ssp :  KO
       credman :

mimikatz(powershell) # exit
Bye!
"


Context:
        Severity = Informational
        Host Name = ConsoleHost
        Host Version = 5.0.10586.0
        Host ID = a6c7f245-168f-4851-9fbe-cf60a584b97d
        Host Application = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
        Engine Version = 5.0.10586.0
        Runspace ID = 1ef18b12-f186-4eed-a5f6-f25af77ffd41
        Pipeline ID = 18
        Command Name =
        Command Type = Script
        Script Name =
        Command Path =
        Sequence Number = 14064
        User = DESKTOP-RMJCHH3\me
        Connected User =
        Shell ID = Microsoft.PowerShell


User Data:
```

Figure 3: `Invoke-Mimikatz` Module Logging Example