Create Ssh.yml #211

New issue

Merged **bohops** merged 3 commits into `LOLBAS-Project:master` from `febou92:patch-1` on Dec 30, 2022

Conversation 1 | Commits 3 | Checks 0 | Files changed

Changes from **all commits** | File filter | Conversations | Jump to

16 yml/OSBinaries/Ssh.yml

```
...  ...  @@ -1,4 +1,3 @@
1       - ---
2    1     Name: ssh.exe
3    2     Description: Ssh.exe is the OpenSSH compatible client can be used to connect to Windows 10
           (build 1809 and later) and Windows Server 2019 devices.
4    3     Author: 'Akshat Pradhan'
     @@ -11,18 +10,21 @@ Commands:
11   10        Privileges: User
12   11        MitreID: T1202
13   12        OperatingSystem: Windows 10 1809, Windows Server 2019
14      -    - Command: ssh localhost calc.exe
15      -      Description: Executes calc.exe.
16      -      Usecase: Performs execution of specified file, can be used to bypass Application
           Whitelisting.
17      -      Category: AWL Bypass
        13  +    - Command: ssh -o ProxyCommand=calc.exe .
        14  +      Description: Executes calc.exe from ssh.exe
        15  +      Usecase: Performs execution of specified file, can be used as a defensive evasion.
        16  +      Category: Execute
18   17        Privileges: User
19      -      MitreID: T1218
20      -      OperatingSystem: Windows 10 1809, Windows Server 2019
```

```
                18  +     MitreID: T1202
                19  +     OperatingSystem: Windows 10
21              20      Full_Path:
22              21        - Path: c:\windows\system32\OpenSSH\ssh.exe
23              22      Detection:
24              23        - Sigma:
                          https://github.com/SigmaHQ/sigma/blob/197615345b927682ab7ad7fa3c5f5bb2ed911eed/rules/windo
                          ws/process_creation/proc_creation_win_lolbin_ssh.yml
25              24        - IOC: Event ID 4624 with process name C:\Windows\System32\OpenSSH\sshd.exe.
26              25        - IOC: command line arguments specifying execution.
                26  + Resources:
                27  +   - Link: https://gtfobins.github.io/gtfobins/ssh/
27              28      Acknowledgement:
28              29        - Person: Akshat Pradhan
                30  +   - Person: Felix Boulet
```