Deep Blue: RDP Compromise and Meterpreter Incident Investigation

Interactive Threat Hunting • Windows Log Analysis • DeepBlueCLI Project

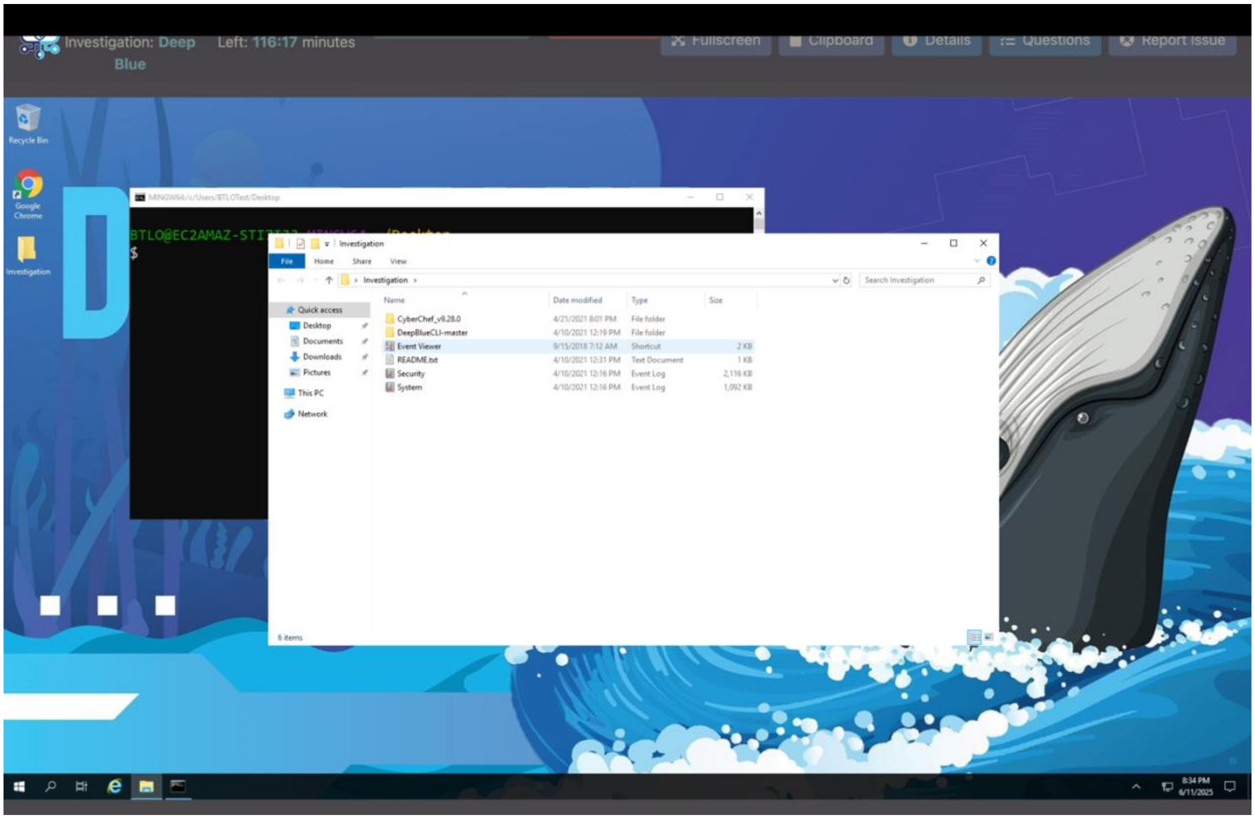
---

Project Overview

This investigation confirmed that a Windows workstation was compromised via an internet-facing RDP service, leading to the deployment of a Meterpreter payload and the creation of persistence mechanisms.

Tools Used:

- DeepBlueCLI (PowerShell)
- Event Viewer
- Command Line Interface (CLI)



```
BTLO@EC2AMAZ-STI
$
```

Name	Date modified	Type	Size
CyberChef_v9.28.0	4/21/2021 8:01 PM	File folder	
DeepBlueCLI-master	4/10/2021 12:19 PM	File folder	
Event Viewer	9/15/2018 7:12 AM	Shortcut	2 KB
README.txt	4/10/2021 12:31 PM	Text Document	1 KB
Security	4/10/2021 12:16 PM	Event Log	2,116 KB
System	4/10/2021 12:16 PM	Event Log	1,092 KB

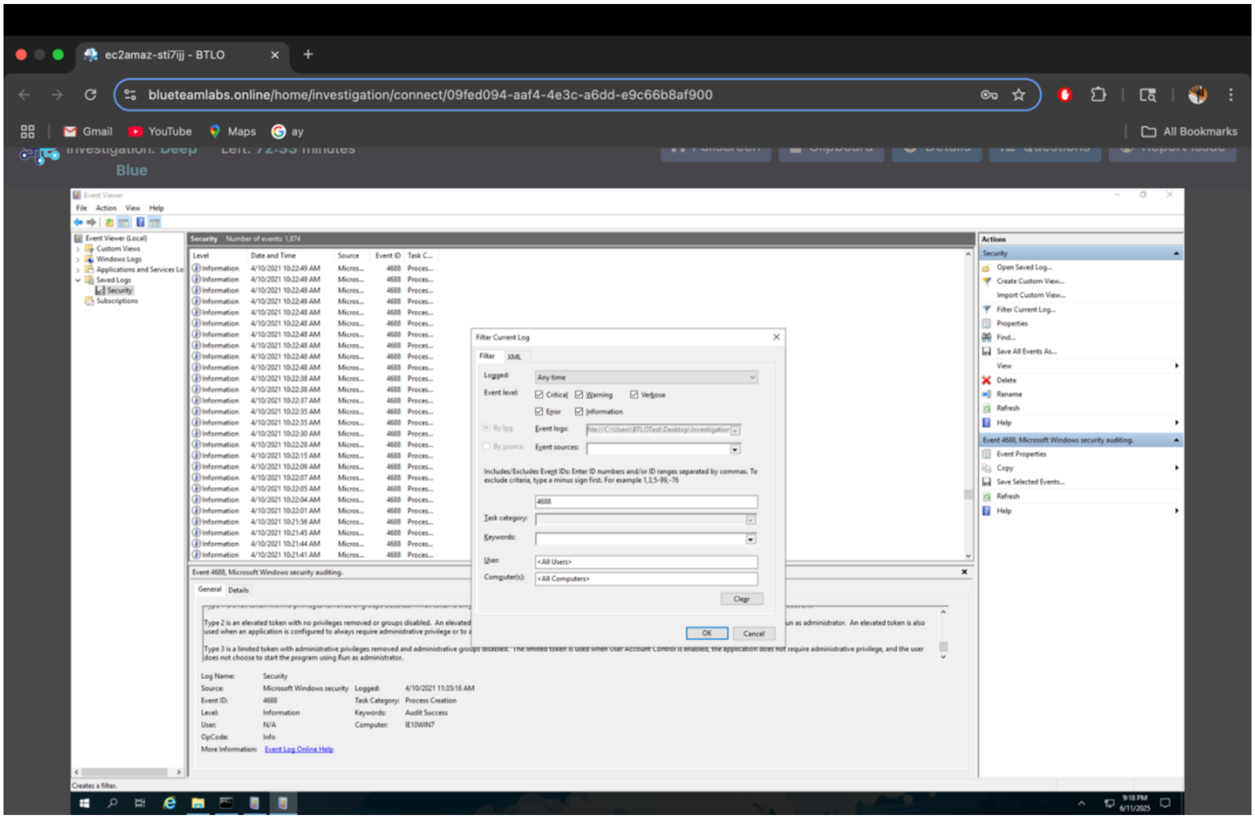
Evidence Collected

- `Security.evtx` – Windows Security Log
- `System.evtx` – Windows System Log

Step 1: Log Loading and Filtering

Security Log:

- Loaded `Security.evtx` in Event Viewer.
- Applied filter:
    - **Event Levels:** Critical, Warning, Verbose, Error, Information
    - **Event ID:** 4688 (Process Creation)



Security Number of events: 1,874

Level	Date and Time	Source	Event ID	Task C...
Information	4/10/2021 10:22:49 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:49 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:49 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:49 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:48 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:48 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:48 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:48 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:48 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:48 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:38 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:38 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:37 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:35 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:35 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:30 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:28 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:15 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:09 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:07 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:05 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:04 AM	Micros...	4688	Proces...
Information	4/10/2021 10:22:01 AM	Micros...	4688	Proces...
Information	4/10/2021 10:21:56 AM	Micros...	4688	Proces...
Information	4/10/2021 10:21:45 AM	Micros...	4688	Proces...
Information	4/10/2021 10:21:44 AM	Micros...	4688	Proces...
Information	4/10/2021 10:21:41 AM	Micros...	4688	Proces...

Filter Current Log

Filter | XML

Logged: Any time

Event level: ☑ Critical ☑ Warning ☑ Verbose ☑ Error ☑ Information

● By log Event logs: file://C:\Users\BTLOTest\Desktop\Investigation

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4688

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Clear

OK Cancel

Event 4688, Microsoft Windows security auditing.

General | Details

Type 2 is an elevated token with no privileges removed or groups disabled. An elevated … un as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to a…

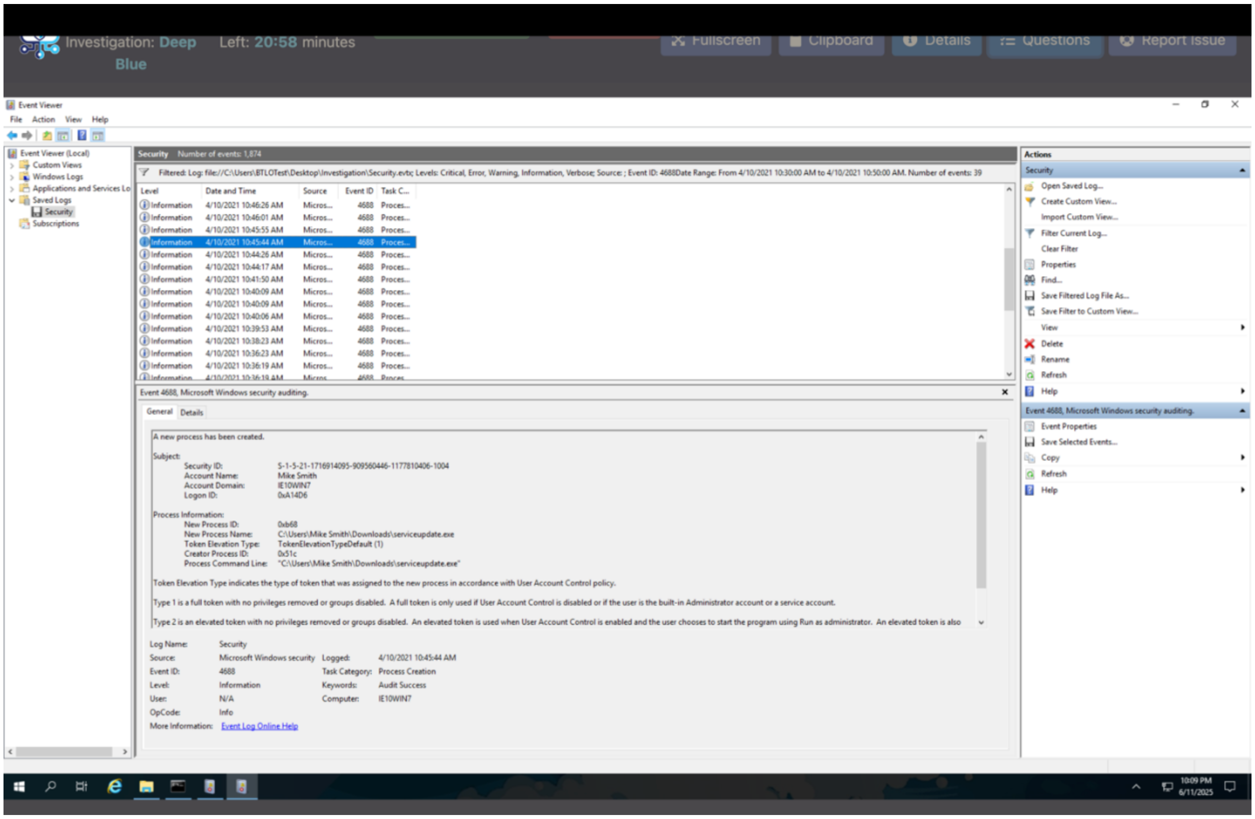
Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	4/10/2021 11:35:16 AM
Event ID:	4688	Task Category:	Process Creation
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	IE10WIN7
OpCode:	Info		
More Information:	Event Log Online Help		

Step 2: Threat Hunting & Key Findings

Finding 1: Malicious Executable Download

- **Malicious File:** `serviceupdate.exe`
- **Execution Time:** 10:48:14 AM, 10 April 2021
- **Executed By:** Mike Smith
- **Event ID:** 4688
- **MITRE Mapping:**
    - Execution: T1059 (Command and Scripting Interpreter)
    - Remote Access: T1071 (Application Layer Protocol)



Security Number of events: 1,874

Filtered: Log: file://C:\Users\BTLOTest\Desktop\Investigation\Security.evtx; Levels: Critical, Error, Warning, Information, Verbose; Source: ; Event ID: 4688Date Range: From 4/10/2021 10:30:00 AM to 4/10/2021 10:50:00 AM. Number of events: 39

```
Level        Date and Time           Source     Event ID  Task C...
Information  4/10/2021 10:46:26 AM   Micros...      4688  Proces...
Information  4/10/2021 10:46:01 AM   Micros...      4688  Proces...
Information  4/10/2021 10:45:55 AM   Micros...      4688  Proces...
Information  4/10/2021 10:45:44 AM   Micros...      4688  Proces...
Information  4/10/2021 10:44:26 AM   Micros...      4688  Proces...
Information  4/10/2021 10:44:17 AM   Micros...      4688  Proces...
Information  4/10/2021 10:41:50 AM   Micros...      4688  Proces...
Information  4/10/2021 10:40:09 AM   Micros...      4688  Proces...
Information  4/10/2021 10:40:09 AM   Micros...      4688  Proces...
Information  4/10/2021 10:40:06 AM   Micros...      4688  Proces...
Information  4/10/2021 10:39:53 AM   Micros...      4688  Proces...
Information  4/10/2021 10:38:23 AM   Micros...      4688  Proces...
Information  4/10/2021 10:36:23 AM   Micros...      4688  Proces...
Information  4/10/2021 10:36:19 AM   Micros...      4688  Proces...
Information  4/10/2021 10:36:19 AM   Micros...      4688  Proces...
```

Event 4688, Microsoft Windows security auditing.

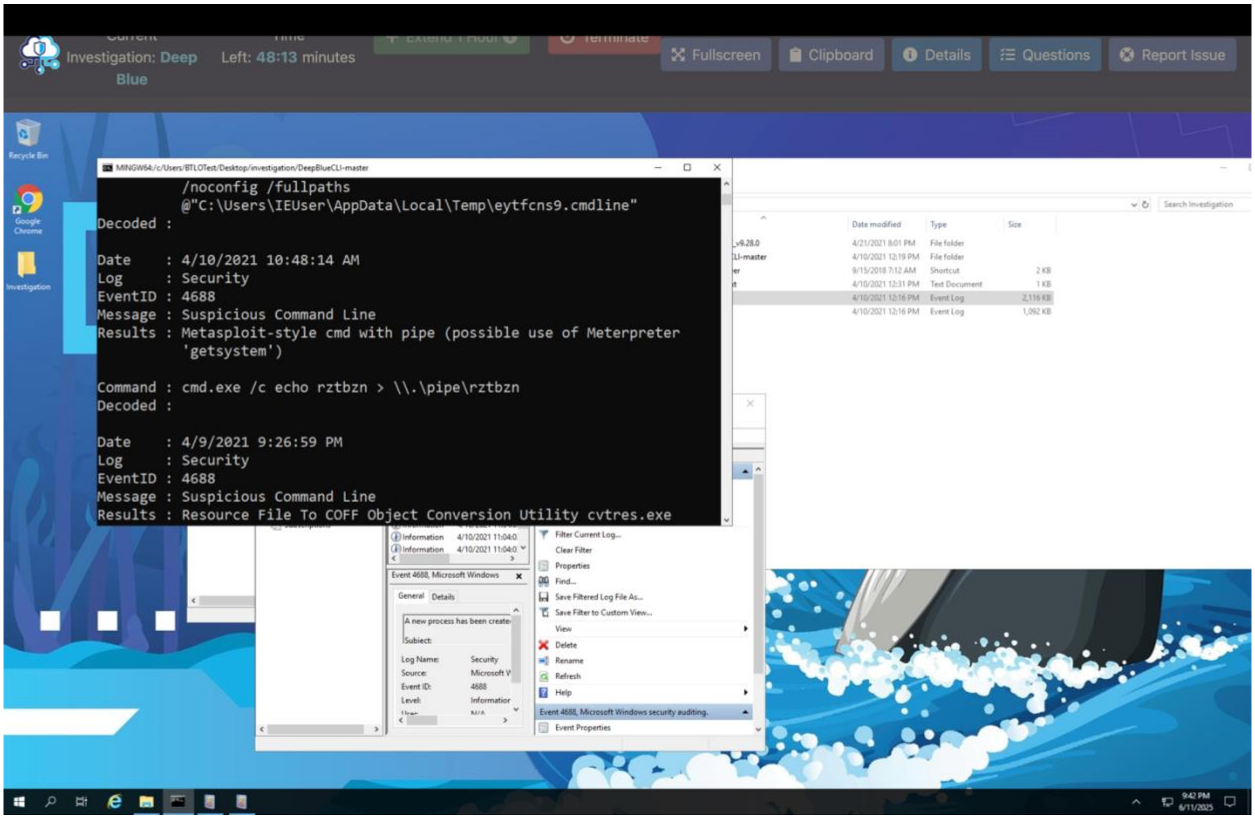
General Details

```
A new process has been created.

Subject:
        Security ID:            S-1-5-21-1716914095-909560446-1177810406-1004
        Account Name:           Mike Smith
        Account Domain:         IE10WIN7
        Logon ID:               0xA14D6

Process Information:
        New Process ID:         0xb68
        New Process Name:       C:\Users\Mike Smith\Downloads\serviceupdate.exe
        Token Elevation Type:   TokenElevationTypeDefault (1)
        Creator Process ID:     0x51c
        Process Command Line:   "C:\Users\Mike Smith\Downloads\serviceupdate.exe"

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled.  A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Type 2 is an elevated token with no privileges removed or groups disabled.  An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator.  An elevated token is also
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          4/10/2021 10:45:44 AM
Event ID:          4688                         Task Category:   Process Creation
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        IE10WIN7
OpCode:            Info
More Information:  Event Log Online Help
```

Finding 2: Meterpreter Activity

- **Evidence of Meterpreter:**
- **Detected Time:** 10:48:14 AM, 10 April 2021
- **Tool Used:** DeepBlueCLI
- **MITRE Mapping:**
    - Command and Control: T1071
    - Exploit Public-Facing Application: T1190



```
         /noconfig /fullpaths
         @"C:\Users\IEUser\AppData\Local\Temp\eytfcns9.cmdline"
Decoded :

Date    : 4/10/2021 10:48:14 AM
Log     : Security
EventID : 4688
Message : Suspicious Command Line
Results : Metasploit-style cmd with pipe (possible use of Meterpreter
          'getsystem')

Command : cmd.exe /c echo rztbzn > \\.\pipe\rztbzn
Decoded :

Date    : 4/9/2021 9:26:59 PM
Log     : Security
EventID : 4688
Message : Suspicious Command Line
Results : Resource File To COFF Object Conversion Utility cvtres.exe
```

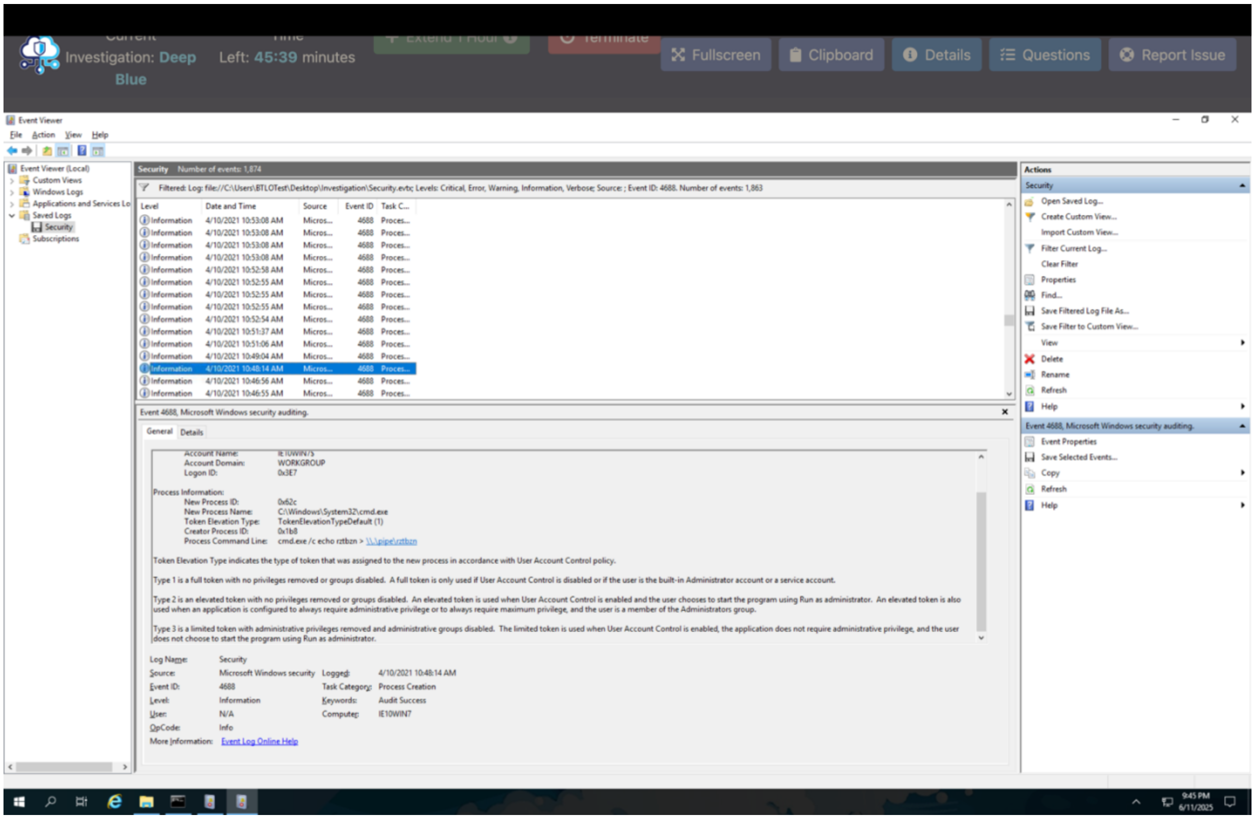
A new process has been create

Subject:

Log Name: Security
Source: Microsoft W
Event ID: 4688
Level: Informatior

Finding 3: Suspicious Service Creation

- **Service Name:** rztbn
- **Event Log:** System.evtx
- **MITRE Mapping:**
  - Persistence: T1543.003 (Create or Modify System Process: Windows Service)



[redacted]

Security Number of events: 1,874

Filtered: Log: file://C:\Users\BTLOTest\Desktop\Investigation\Security.evtx; Levels: Critical, Error, Warning, Information, Verbose; Source: ; Event ID: 4688. Number of events: 1,863

Level	Date and Time	Source	Event ID	Task C...
Information	4/10/2021 10:53:08 AM	Micros...	4688	Proces...
Information	4/10/2021 10:53:08 AM	Micros...	4688	Proces...
Information	4/10/2021 10:53:08 AM	Micros...	4688	Proces...
Information	4/10/2021 10:53:08 AM	Micros...	4688	Proces...
Information	4/10/2021 10:52:58 AM	Micros...	4688	Proces...
Information	4/10/2021 10:52:55 AM	Micros...	4688	Proces...
Information	4/10/2021 10:52:55 AM	Micros...	4688	Proces...
Information	4/10/2021 10:52:55 AM	Micros...	4688	Proces...
Information	4/10/2021 10:52:54 AM	Micros...	4688	Proces...
Information	4/10/2021 10:51:37 AM	Micros...	4688	Proces...
Information	4/10/2021 10:51:06 AM	Micros...	4688	Proces...
Information	4/10/2021 10:49:04 AM	Micros...	4688	Proces...
Information	4/10/2021 10:48:14 AM	Micros...	4688	Proces...
Information	4/10/2021 10:46:56 AM	Micros...	4688	Proces...
Information	4/10/2021 10:46:55 AM	Micros...	4688	Proces...

Event 4688, Microsoft Windows security auditing.

General Details

```
        Account Name:           IE10WIN7$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Process Information:
        New Process ID:         0x62c
        New Process Name:       C:\Windows\System32\cmd.exe
        Token Elevation Type:   TokenElevationTypeDefault (1)
        Creator Process ID:     0x1b8
        Process Command Line:   cmd.exe /c echo rztbzn > \\.\pipe\rztbzn
```

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group.

Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

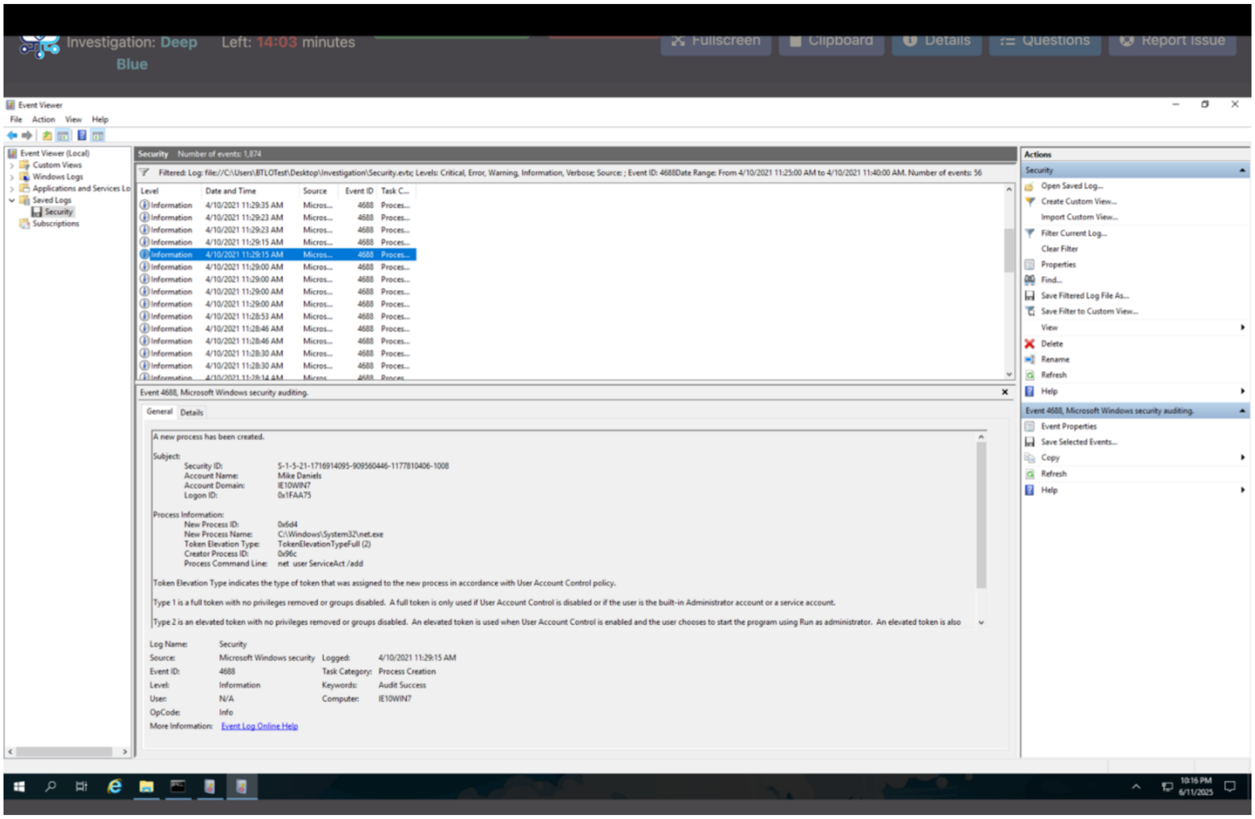
Log Name:	Security		
Source:	Microsoft Windows security	Logged:	4/10/2021 10:48:14 AM
Event ID:	4688	Task Category:	Process Creation
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	IE10WIN7
OpCode:	Info		
More Information:	Event Log Online Help		

Finding 4: Persistence Account Creation

- **Command Executed:**

  ```
  net user ServiceAct /add
  ```

- **Timeframe:** Between 11:25 AM and 11:40 AM, 10 April 2021
- **Event Log:** Security.evtx



Security Number of events: 1,874

Filtered: Log: file://C:\Users\BTLOTest\Desktop\Investigation\Security.evtx; Levels: Critical, Error, Warning, Information, Verbose; Source: ; Event ID: 4688Date Range: From 4/10/2021 11:25:00 AM to 4/10/2021 11:40:00 AM. Number of events: 56

Level	Date and Time	Source	Event ID	Task C...
Information	4/10/2021 11:29:35 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:23 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:23 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:15 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:15 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:00 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:00 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:00 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:00 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:53 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:46 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:46 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:30 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:30 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:14 AM	Micros...	4688	Proces...

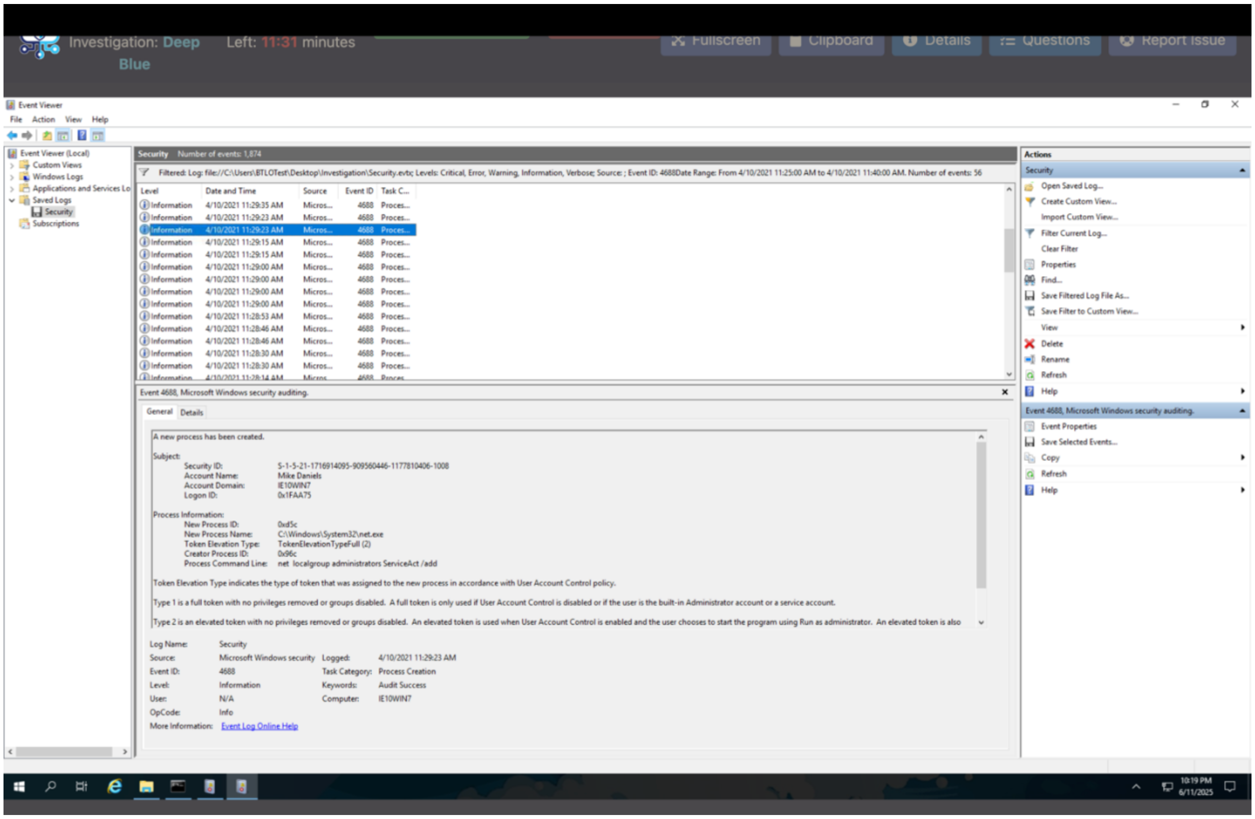
Event 4688, Microsoft Windows security auditing.

```
A new process has been created.

Subject:
        Security ID:            S-1-5-21-1716914095-909560446-1177810406-1008
        Account Name:           Mike Daniels
        Account Domain:         IE10WIN7
        Logon ID:               0x1FAA75

Process Information:
        New Process ID:         0x6d4
        New Process Name:       C:\Windows\System32\net.exe
        Token Elevation Type:   TokenElevationTypeFull (2)
        Creator Process ID:     0x96c
        Process Command Line:   net  user ServiceAct /add

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled.  A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Type 2 is an elevated token with no privileges removed or groups disabled.  An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator.  An elevated token is also
```

```
Log Name:          Security
Source:            Microsoft Windows security    Logged:          4/10/2021 11:29:15 AM
Event ID:          4688                          Task Category:   Process Creation
Level:             Information                   Keywords:        Audit Success
User:              N/A                           Computer:        IE10WIN7
OpCode:            Info
More Information:  Event Log Online Help
```

Local Groups Added:

- Administrators
- Remote Desktop Users
- **MITRE Mapping:**
  - Create Account: T1136.001 (Local Account)
  - Privilege Escalation: T1078.003 (Local Accounts)



Security Number of events: 1,874

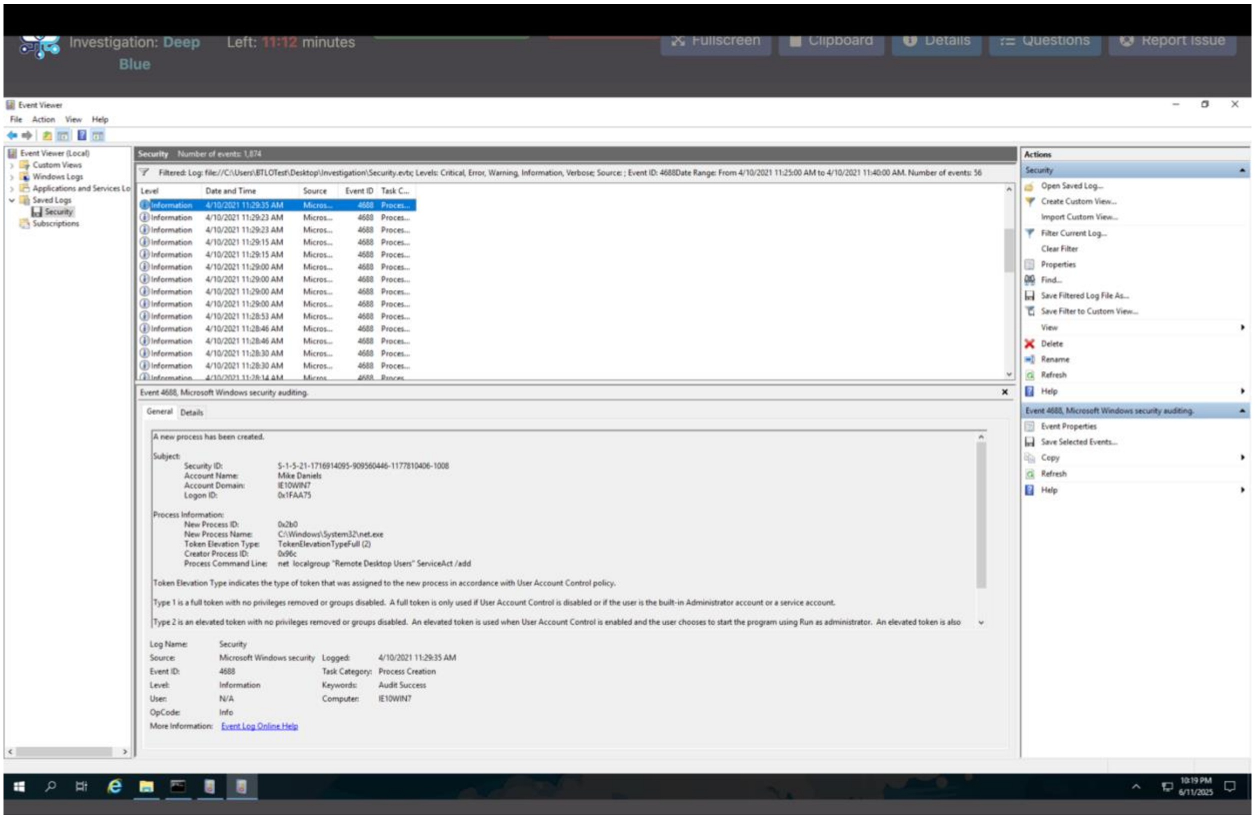
Filtered: Log: file://C:\Users\BTLOTest\Desktop\Investigation\Security.evtx; Levels: Critical, Error, Warning, Information, Verbose; Source: ; Event ID: 4688Date Range: From 4/10/2021 11:25:00 AM to 4/10/2021 11:40:00 AM. Number of events: 56

Level	Date and Time	Source	Event ID	Task C...
Information	4/10/2021 11:29:35 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:23 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:23 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:15 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:15 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:00 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:00 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:00 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:00 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:53 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:46 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:46 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:30 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:30 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:14 AM	Micros...	4688	Proces...

Event 4688, Microsoft Windows security auditing.

```
A new process has been created.

Subject:
        Security ID:            S-1-5-21-1716914095-909560446-1177810406-1008
        Account Name:           Mike Daniels
        Account Domain:         IE10WIN7
        Logon ID:               0x1FAA75

Process Information:
        New Process ID:         0xd5c
        New Process Name:       C:\Windows\System32\net.exe
        Token Elevation Type:   TokenElevationTypeFull (2)
        Creator Process ID:     0x96c
        Process Command Line:   net  localgroup administrators ServiceAct /add

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled.  A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Type 2 is an elevated token with no privileges removed or groups disabled.  An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator.  An elevated token is also
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	4/10/2021 11:29:23 AM
Event ID:	4688	Task Category:	Process Creation
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	IE10WIN7
OpCode:	Info		
More Information:	Event Log Online Help		



Security Number of events: 1,874

Filtered: Log: file://C:\Users\BTLOTest\Desktop\Investigation\Security.evtx; Levels: Critical, Error, Warning, Information, Verbose; Source: ; Event ID: 4688Date Range: From 4/10/2021 11:25:00 AM to 4/10/2021 11:40:00 AM. Number of events: 56

Level	Date and Time	Source	Event ID	Task C...
Information	4/10/2021 11:29:35 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:23 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:23 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:15 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:15 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:00 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:00 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:00 AM	Micros...	4688	Proces...
Information	4/10/2021 11:29:00 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:53 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:46 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:46 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:30 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:30 AM	Micros...	4688	Proces...
Information	4/10/2021 11:28:14 AM	Micros...	4688	Proces...

Event 4688, Microsoft Windows security auditing.

```
A new process has been created.

Subject:
        Security ID:            S-1-5-21-1716914095-909560446-1177810406-1008
        Account Name:           Mike Daniels
        Account Domain:         IE10WIN7
        Logon ID:               0x1FAA75

Process Information:
        New Process ID:         0x2b0
        New Process Name:       C:\Windows\System32\net.exe
        Token Elevation Type:   TokenElevationTypeFull (2)
        Creator Process ID:     0x96c
        Process Command Line:   net  localgroup "Remote Desktop Users" ServiceAct /add

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled.  A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.

Type 2 is an elevated token with no privileges removed or groups disabled.  An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator.  An elevated token is also
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	4/10/2021 11:29:35 AM
Event ID:	4688	Task Category:	Process Creation
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	IE10WIN7
OpCode:	Info		
More Information:	Event Log Online Help		

📅 Timeline of Attack

Time	Event Description	Log Source	MITRE Technique
10:48:14 AM	serviceupdate.exe executed by Mike Smith	Security.evtx	T1059
10:48:14 AM	Meterpreter likely deployed	Security.evtx	T1071
~11:30 AM	Backdoor account created: serviceact	Security.evtx	T1136.001
~11:35 AM	Account added to Administrators & RDP groups	Security.evtx	T1078.003
~11:36 AM	Suspicious service created: rztbn	System.evtx	T1543.003

Defense Recommendations

- **Disable public-facing RDP or restrict access via VPN.**
- **Enforce Multi-Factor Authentication (MFA) for all remote logins.**
- **Continuously monitor Event IDs:**
  - 4688 (Process Creation)
  - 4624 (Successful Login)
  - Service creation events
- **Proactively hunt with DeepBlueCLI to detect abnormal PowerShell and Meterpreter activity.**

Final Reflection

This hands-on investigation solidified my skills in:
✅ Windows Event Log analysis
✅ DeepBlueCLI threat hunting
✅ Timeline-based incident reconstruction
✅ Practical MITRE ATT&CK mapping

Pro Tip: Cross-check all logs using CLI and DeepBlueCLI to ensure no artifacts are overlooked. A layered approach is key to catching stealthy attacker behaviors.
