Suspicious Local User Creation and Privilege Abuse

1 message

<rangammabokka46@gmail.com> Sat, May 24, 2025 at 9:04 PM
Reply-to: rangammabokka46@gmail.com
To: rangammabokka46@gmail.com

A new local user was created and added to the administrators group.

At least 1 events occurred between 2025-05-24 20:43 India Standard Time and 2025-05-24 20:53 India Standard Time

```
@timestamp: 2025-05-24T15:23:19.574Z
_id: 4EzkApcBju6GhRx1QNCJ
_index: .ds-winlogbeat-8.10.2-2025.05.14-000001
agent: {
  "ephemeral_id": "e554b7b3-41cc-4d4b-82ad-de9408b80f6f",
  "id": "e5e3a761-acc3-41a2-88c5-ee2b2b236970",
  "name": "Viticm-SOC",
  "type": "winlogbeat",
  "version": "8.10.2"
}
ecs: {
  "version": "1.12.0"
}
event: {
  "action": "added-user-account",
  "category": [
    "iam"
  ],
  "code": "4720",
  "created": "2025-05-24T15:23:23.076Z",
  "ingested": "2025-05-24T15:23:22.584704800Z",
  "kind": "event",
  "module": "security",
  "outcome": "success",
  "provider": "Microsoft-Windows-Security-Auditing",
  "type": [
    "user",
    "creation"
  ]
}
host: {
  "architecture": "x86_64",
  "hostname": "viticm-soc",
  "id": "7e25c1a1-4745-47c6-abe9-ec7f50bf1d98",
  "ip": [
    "fe80::2674:6aaf:881:b09b",
    "192.168.52.131"
  ],
  "mac": [
    "00-0C-29-C5-7F-10"
  ],
  "name": "viticm-soc",
  "os": {
    "build": "19045.5854",
    "family": "windows",
    "kernel": "10.0.19041.5848 (WinBuild.160101.0800)",
    "name": "Windows 10 Home",
    "platform": "windows",
    "type": "windows",
    "version": "10.0"
  }
}
log: {
  "level": "information"
}
message: A user account was created.
```

```
Subject:
	Security ID:		S-1-5-21-3403377879-2231786425-1901733960-1001
	Account Name:		ranga
	Account Domain:		VITICM-SOC
	Logon ID:		0x55FBA

New Account:
	Security ID:		S-1-5-21-3403377879-2231786425-1901733960-1002
	Account Name:		attacker
	Account Domain:		VITICM-SOC

Attributes:
	SAM Account Name:	attacker
	Display Name:		<value not set>
	User Principal Name:	-
	Home Directory:		<value not set>
	Home Drive:		<value not set>
	Script Path:		<value not set>
	Profile Path:		<value not set>
	User Workstations:	<value not set>
	Password Last Set:	<never>
	Account Expires:		<never>
	Primary Group ID:	513
	Allowed To Delegate To:	-
	Old UAC Value:		0x0
	New UAC Value:		0x15
	User Account Control:	
		Account Disabled
		'Password Not Required' - Enabled
		'Normal Account' - Enabled
	User Parameters:	<value not set>
	SID History:		-
	Logon Hours:		All

Additional Information:
	Privileges		-
num_hits: 3
num_matches: 3
related: {
  "user": [
    "ranga",
    "attacker"
  ]
}
user: {
  "domain": "VITICM-SOC",
  "id": "S-1-5-21-3403377879-2231786425-1901733960-1001",
  "name": "ranga",
  "target": {
    "domain": "VITICM-SOC",
    "id": "S-1-5-21-3403377879-2231786425-1901733960-1002",
    "name": "attacker"
  }
}
winlog: {
  "activity_id": "{fad47bef-ccb5-0000-da7d-d4fab5ccdb01}",
  "api": "wineventlog",
  "channel": "Security",
  "computer_name": "Viticm-SOC",
  "event_data": {
    "AccountExpires": "%%1794",
    "AllowedToDelegateTo": "-",
    "DisplayName": "%%1793",
    "HomeDirectory": "%%1793",
    "HomePath": "%%1793",
    "LogonHours": "%%1797",
    "NewUACList": [
      "SCRIPT",
      "LOCKOUT"
    ],
    "NewUacValue": "0x15",
    "OldUacValue": "0x0",
    "PasswordLastSet": "%%1794",
    "PrimaryGroupId": "513",
        "PrivilegeList": "-",
        "ProfilePath": "%%1793",
        "SamAccountName": "attacker",
        "ScriptPath": "%%1793",
        "SidHistory": "-",
        "SubjectDomainName": "VITICM-SOC",
        "SubjectLogonId": "0x55fba",
        "SubjectUserName": "ranga",
        "SubjectUserSid": "S-1-5-21-3403377879-2231786425-1901733960-1001",
        "TargetDomainName": "VITICM-SOC",
        "TargetSid": "S-1-5-21-3403377879-2231786425-1901733960-1002",
        "TargetUserName": "attacker",
        "UserAccountControl": [
            "2080",
            "2082",
            "2084"
        ],
        "UserParameters": "%%1793",
        "UserPrincipalName": "-",
        "UserWorkstations": "%%1793"
    },
    "event_id": "4720",
    "keywords": [
        "Audit Success"
    ],
    "logon": {
        "id": "0x55fba"
    },
    "opcode": "Info",
    "process": {
        "pid": 828,
        "thread": {
            "id": 3384
        }
    },
    "provider_guid": "{54849625-5478-4994-a5ba-3e3b0328c30d}",
    "provider_name": "Microsoft-Windows-Security-Auditing",
    "record_id": "64617",
    "task": "User Account Management"
}
```