C2 Beacon

Time	Event
2025-06-13T16:34:54+0530	06/13/2025 04:34:54 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113557 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:50:59.656 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65184 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http
2025-06-13T16:34:34+0530	06/13/2025 04:34:34 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113556 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:50:39.624 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65179 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http

Time	Event
2025-06-13T16:34:15+0530	06/13/2025 04:34:15 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113555 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:50:19.610 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65175 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http
2025-06-13T16:33:54+0530	06/13/2025 04:33:54 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113548 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:49:59.578 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65172 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http

Time	Event
2025-06-13T16:33:35+0530	06/13/2025 04:33:35 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113547 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:49:39.563 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65167 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http
2025-06-13T16:33:15+0530	06/13/2025 04:33:15 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113546 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:49:19.530 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65163 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http

Time	Event
2025-06-13T16:32:54+0530	06/13/2025 04:32:54 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113539 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:48:59.515 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65161 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http
2025-06-13T16:32:35+0530	06/13/2025 04:32:35 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113538 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:48:39.500 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65155 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http

Time	Event
2025-06-13T16:32:15+0530	06/13/2025 04:32:15 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113537 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:48:19.469 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65151 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http
2025-06-13T16:31:55+0530	06/13/2025 04:31:55 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113530 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:47:59.437 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65146 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http

Time	Event
2025-06-13T16:31:35+0530	06/13/2025 04:31:35 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113529 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:47:39.422 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65142 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http
2025-06-13T16:31:14+0530	06/13/2025 04:31:14 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113528 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:47:19.405 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65139 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http

Time	Event
2025-06-13T16:30:54+0530	06/13/2025 04:30:54 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113521 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:46:59.391 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65130 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http
2025-06-13T16:30:34+0530	06/13/2025 04:30:34 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113520 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:46:39.389 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65116 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http

Time	Event
2025-06-13T16:30:15+0530	06/13/2025 04:30:15 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113519 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:46:19.375 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65104 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http
2025-06-13T16:29:54+0530	06/13/2025 04:29:54 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113518 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:45:59.359 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65091 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http

Time	Event
2025-06-13T16:29:34+0530	06/13/2025 04:29:34 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113517 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:45:39.342 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65078 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http
2025-06-13T16:29:14+0530	06/13/2025 04:29:14 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113514 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:45:19.327 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65065 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http

Time	Event
2025-06-13T16:28:54+0530	06/13/2025 04:28:54 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113512 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:44:59.312 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65055 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http
2025-06-13T16:28:34+0530	06/13/2025 04:28:34 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=113511 Keywords=None TaskCategory=Network connection detected (rule: NetworkConnect) OpCode=Info Message=Network connection detected: RuleName: - UtcTime: 2025-06-13 10:44:39.296 ProcessGuid: {a9155468-00bd-684c-d904-000000003a00} ProcessId: 12628 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-F049LOK\suver Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.246.129 SourceHostname: DESKTOP-F049LOK.localdomain SourcePort: 65043 SourcePortName: - DestinationIsIpv6: false DestinationIp: 192.168.246.131 DestinationHostname: - DestinationPort: 80 DestinationPortName: http