Executive Summary:

On February 8, 2024, a series of suspicious network activities were identified within the LAN segment 10.2.8.0/24 under the domain ascolimited.com. These activities originated from the host "DESKTOP-MGVG60Z" with the IP address 10.2.8.101, associated with the Windows user account "bill.cook." Notably, this host engaged in connections with various external IP addresses, including communication with Command and Control (C2) servers. Furthermore, it was observed that the host initiated downloads of potentially harmful executables via HTTP requests, signaling a significant security threat within the network infrastructure.

Detailed Analysis:

The compromised device, identified as DESKTOP-MGVG60Z, possesses the IP address 10.2.8.101 and MAC address 00:12:79:41:c2:aa. The Windows user account linked to this system is "bill.cook." These specifics furnish essential insights into the affected machine's identity and potential vulnerabilities.

Indicators of Compromise:

To facilitate the detection of similar incursions, critical details have been shown: the IPs of Command and Control servers are 213.5.229.12, 198.211.10.238, and 185.100.65.29. The initial exploit was conducted through the host roanokemortgages.com, which was discovered to be harboring malicious files, specifically: /0801.bin, /0801s.bin, and /6lhjgfdghj.exe.

Examining the data captured in WireShark, specific packets reveal pertinent information:

Packet 3880:
Host: roanokemortgages.com
URL: GET /0801.bin HTTP/1.1
IP address: 8.208.10.147
MAC Address: 00:12:79:41:c2:aa
Source IP Address: 10.2.8.101

Packet 3884:
Host: roanokemortgages.com
URL: GET /0801s.bin HTTP/1.1
IP address: 8.208.10.147

Packet 3910:
Host: roanokemortgages.com
URL: GET /6lhjgfdghj.exe
IP address: 8.208.10.147

DESKTOP-MGVG60Z Registrations:

A series of network registrations further emphasize the involvement of DESKTOP-MGVG60Z within the compromised network environment. These registrations include:

Source	Destination	Protocol	Length	Info
10.2.8.101	10.2.8.255	NBNS	110	Registration NB DESKTOP-MGVG60Z<20>
10.2.8.101	10.2.8.255	NBNS	110	Registration NB DESKTOP-MGVG60Z<00>
10.2.8.101	10.2.8.255	NBNS	110	Registration NB DESKTOP-MGVG60Z<20>
10.2.8.101	10.2.8.255	NBNS	110	Registration NB DESKTOP-MGVG60Z<00>
10.2.8.101	10.2.8.255	NBNS	110	Registration NB DESKTOP-MGVG60Z<00>
10.2.8.101	10.2.8.255	NBNS	110	Registration NB DESKTOP-MGVG60Z<20>
10.2.8.101	10.2.8.255	NBNS	110	Registration NB DESKTOP-MGVG60Z<00>
10.2.8.101	10.2.8.255	NBNS	110	Registration NB DESKTOP-MGVG60Z<20>

Windows User Account: 10.2.8.101 (DESKTOP-MGVG60Z) bill.cook

3 Files:

- 0801.bin

- 0801s.bin

- 6lhjgfdghj.exe

In conclusion, the infiltration of the network by the host DESKTOP-MGVG60Z under the guise of the Windows user account "bill.cook" presents a grave security concern. Action must be taken promptly to mitigate the potential risks posed by the observed malicious activity.