Universe International Journal of Interdisciplinary Research
(International Peer Reviewed Refereed Journal)
DOI No. – 08.2020-25662434

OCT 2025 | Vol. 06 Issue 05
www.uijir.com

CONTROL OVER A ROUTER VIA ARP COVERT CHANNEL

Author's Name: Akor Jacob Terungwa [1]

Affiliation:

1. Student, Innopolis University, Russia.

Corresponding Author Name & Email Id: Akor Jacob Terungwa,
akorjacob54@gmail.com

ABSTRACT

The study utilized an action research approach wherein the researcher used PowerPoint Slide The increasing sophistication of cyberattacks has encouraged adversaries to exploit covert communication channels that evade conventional security controls. This study explores the feasibility of using the Address Resolution Protocol (ARP) as a covert command-and-control (C2) channel for MikroTik routers. Leveraging ARP's lack of authentication, encryption, and logging, a proof-of-concept was developed in a controlled GNS3 environment. A Python client injected commands into spoofed MAC address fields of ARP packets, while a MikroTik script monitored its ARP table and executed actions including rebooting, DNS spoofing, and reverting spoofing. The approach successfully established covert communication that bypassed common defenses such as firewalls and DNS monitoring. Mitigation strategies using Wazuh and Zeek demonstrated effective detection of anomalies. The findings highlight ARP-based covert channels as a practical Layer 2 security risk and propose viable detection mechanisms.

Keywords: Covert channel, ARP, MikroTik, Network Security, Layer 2, Wazuh, Zeek, Command and Control (C2)

DOI Link :: https://doi-ds.org/doilink/10.2025-11763429/UIJIR

INTRODUCTION

Cyberattacks have evolved significantly, leveraging covert communication channels that exploit the weaknesses of fundamental network protocols. The Address Resolution Protocol (ARP) is one such protocol susceptible to abuse due to its lack of authentication and encryption. This study investigates the potential of ARP to serve as a covert command and control (C2) mechanism for compromised routers. Routers, being central to network operations, present an appealing target for attackers seeking persistence and stealth. By embedding commands into ARP packets, adversaries can evade traditional network defenses such as firewalls and DNS monitoring. This work demonstrates a practical implementation of such a covert channel and proposes detection strategies to mitigate the threat.

RELATED WORK

Prior studies have identified vulnerabilities in ARP that can be leveraged for spoofing and steganographic purposes. Bedi (2020) introduced ARPNetSteg, enabling covert data transfer through ARP packets. Ovadia et al. (2019) demonstrated cross-router covert channels that bypass security appliances. Schmidbauer (2023) and Lamshöft (2022) analyzed persistent covert channels in Layer 2 protocols, emphasizing the lack of robust inspection mechanisms. While mitigation techniques such as Dynamic ARP Inspection exist, their adoption remains limited. This study builds on these findings by constructing a proof-of-concept ARP covert channel in a simulated environment and evaluating mitigation using Wazuh and Zeek.

METHODOLOGY

The research employed an experimental approach within a controlled GNS3 environment. The setup included an Ubuntu attacker host and a MikroTik Cloud Hosted Router (CHR) as the target device. The attacker executed a Python script utilizing Scapy to craft ARP packets with spoofed MAC addresses. The router executed a MikroTik script that monitored its ARP table for specific MAC addresses mapped to commands such as reboot, DNS spoofing, and undo spoofing. The methodology involved developing the scripts, sending crafted ARP packets, observing router responses, and assessing detection tools such as Wazuh and Zeek.

Table 1 – Mapping of Commands to MAC Addresses

Command	MAC Address
REBOOT	92:F3:FD:8A:A9:AB
DO DNS SPOOF	31:F5:9D:34:BE:0A
UNDO DNS SPOOF	51:F7:AD:44:CE:1B

DOI Link :: https://doi-ds.org/doilink/10.2025-11763429/UIJIR

Snippet 1 – Python Attacker Script

```
from scapy.all import ARP, Ether, sendp

LOOKUP = {
  'REBOOT': '92:F3:FD:8A:A9:AB',
  'DNS_SPOOF': '31:F5:9D:34:BE:0A',
  'UNDO_DNS_SPOOF': '51:F7:AD:44:CE:1B'
}
def send_arp_command(router_ip, iface, command):
  if command not in LOOKUP:
    print('Unknown command')
    return
  spoofed_mac = LOOKUP[command]
  arp = ARP(op=1, pdst=router_ip, hwsrc=spoofed_mac)
  eth = Ether(dst='ff:ff:ff:ff:ff:ff')
  pkt = eth / arp
  sendp(pkt, iface=iface, verbose=False)
  print(f'Command sent: {command}')
```

RESULTS AND DISCUSSION

The implementation successfully demonstrated ARP's capability as a covert communication channel. Commands embedded in spoofed MAC addresses were recognized and executed by the MikroTik router without detection by firewalls or endpoint antivirus. However, the covert channel exhibited limitations such as stateless communication, lack of acknowledgment, and low data capacity due to the six-byte MAC address field. Despite these constraints, the channel maintained functionality in a simulated environment, confirming its viability for covert control.

MITIGATION AND DETECTION

To counter ARP-based covert channels, Dynamic ARP Inspection (DAI) and Layer 2 traffic analysis should be employed. Two open-source tools—Wazuh and Zeek—were integrated to provide detection capabilities. Wazuh performed script auditing on MikroTik devices, alerting administrators to unauthorized script modifications. Zeek monitored ARP traffic for untrusted MAC addresses,

DOI Link :: https://doi-ds.org/doilink/10.2025-11763429/UIJIR

identifying potential command injections. Together, these tools provided a robust multi-layered defense.

Snippet 2 – Zeek Detection Script

```
@load base/protocols/arp/arp
module CovertARP; ·
const trusted_macs: set[string] = {
  '08:00:27:f8:cb:5b', '08:00:27:35:55:75', '08:00:27:24:3b:71'
};
event arp_request(mac_src: string, mac_dst: string, SPA: addr, SHA: string, TPA: addr, THA: string)
{
  if (to_lower(SHA) !in trusted_macs)
    Reporter::info(fmt('Untrusted MAC in ARP: %s', SHA));
}
```

CONCLUSION AND FUTURE WORK

This study established the feasibility of ARP-based covert communication for router control and evaluated detection mechanisms to counter such threats. While the covert channel bypasses traditional defenses, the combination of Wazuh and Zeek proved effective in detecting anomalies. Future work should explore stateful command exchange, MAC address obfuscation, and hybrid covert channels using multiple protocols. Enhanced monitoring of Layer 2 traffic is critical for mitigating these emerging risks.

REFERENCES

2. Bedi, H.K. (2020). Network Steganography using Address Resolution Protocol. International Journal of Computer Science and Network Security, 20(6), 75–82.
3. Ovadia, A., et al. (2019). Cross-Router Covert Channels. USENIX Workshop on Offensive Technologies.
4. Schmidbauer, K. (2023). Novel Sophisticated Network-Level Covert Channels. PhD Dissertation, FernUniversität in Hagen.
5. Lamshöft, K. (2022). Threat Analysis, Detection & Mitigation of Covert Channels in Network Systems. Journal of Information Security and Applications, 63, 103163.
6. Nasser, R., & Hussain, F. (2023). Detection and Prevention of ARP Spoofing Attacks in Wireless Networks. IEEE Transactions on Wireless Communications, 22(3), 1410–1422.

DOI Link :: https://doi-ds.org/doilink/10.2025-11763429/UIJIR

7. Mazurczyk, W., Smolarczyk, K., & Szczypiorski, K. (2016). Covert channels in network protocols: survey and taxonomy. IEEE Communications Surveys & Tutorials, 18(2), 1185–1207.

DOI Link :: https://doi-ds.org/doilink/10.2025-11763429/UIJIR