

Fire Ant expands operations to trusted infrastructure

Original report published on: August 27, 2026^[1]

Executive Summary

Active since 2025, Fire Ant has been observed by Sygnia expanding its operations beyond hypervisors to target trusted infrastructure, including routers, Terminal Access Controller Access-Control System (TACACS) authentication systems and Linux management hosts.

Fire Ant compromises network and authentication infrastructure to maintain covert access, capture network traffic and administrative credentials, and identify access paths to connected high-value environments, including critical infrastructure. Compromised routers were also used for traffic collection, covert connectivity and reconnaissance.

The threat actor deployed multiple malware implants for persistence, including BridgeAgent, Medusa-related components, custom SSH backdoors and packet-triggered backdoors while manipulating router and host telemetry to conceal its activities. Sygnia identified strong overlaps between Fire Ant's activities and tooling publicly associated with the UNC3886 cyber espionage threat actor.

Background

Fire Ant has previously compromised VMware ESXi hypervisors, enabling it to operate below the visibility of traditional endpoint security controls. In 2026, the threat actor expanded its operations to infrastructure responsible for routing traffic, authenticating administrators, managing access and recording activity.

Fire Ant was observed compromising Cisco routers and using them as operational platforms for covert connectivity and network reconnaissance. The threat actor established GRE tunnels, conducted network probing against connected environments, captured traffic from multiple routers and transferred PCAP files to external infrastructure.

Additionally, TACACS protocol authentication infrastructure was compromised, allowing Fire Ant to intercept authentication flows and collect administrative credentials. A VMCI/VSOCK-based backdoor was deployed on a TACACS server while malicious modifications to the `tac_plus` process enabled credential collection.

On Linux management infrastructure, Fire Ant deployed persistent malware implants, including BridgeAgent, a backdoor masquerading as a legitimate Zabbix component. BridgeAgent used encrypted configuration, HTTPS-based command-and-control (C2) communications and reverse-shell functionality. Other observed tooling included Medusa-related components, custom SSH backdoors and packet-triggered backdoors.

Fire Ant's defence evasion and anti-forensic techniques included disabling router logs, Authentication, Authorisation and Accounting (AAA) related telemetry and SNMP traps, manipulating command outputs, disabling SELinux, deleting files, modifying firewall rules and tampering with Linux authentication and system logs.

By compromising infrastructure that provides connectivity and administrative trust between environments, Fire Ant could potentially use an initially compromised organisation as a pathway to other connected high-value networks or customer environments.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validation of existing security controls to ensure detection and prevention against the Fire Ant threat activity identified in this advisory:

- Scan for Indicators of Compromise to detect threat activities ([Annex A](#)).
- Refer to the MITRE ATT&CK techniques in this advisory ([Annex B](#)):
 - Create, test and validate detection rules against the threat behaviours.
 - Validate and deny/disable processes, ports and protocols that have no business need.
- Refer to the threat hunting and detection opportunities ([Annex C](#)) to identify and apply relevant detection rules and signatures for ongoing threat monitoring.
- Use NDR capabilities to monitor for anomalous network traffic and detect potential lateral movement across network devices, management systems and other high-value infrastructure.
- Review routers and network devices for unauthorised GRE tunnels, configuration changes, shell access and unexpected traffic captures.
- Monitor for unusual PCAP generation and FTP/SCP transfers from network devices, particularly to external infrastructure.
- Review TACACS/AAA infrastructure for process injection, suspicious credential-related files and administrative activity without corresponding authentication records.
- Review Linux systems for unauthorised disabling of SELinux, suspicious firewall modifications, deleted-but-running processes and unauthorised files within /var/tmp and other temporary directories.
- Monitor for modifications to authentication and system logs, including wtmp, utmp, btmp, lastlog, /var/log/messages and /var/log/secure.
- Restrict administrative access to routers, hypervisors, TACACS servers, jump hosts and management appliances and enforce MFA and least privilege where supported.
- Segment management infrastructure from production and external networks and restrict unnecessary connectivity between trusted administrative environments.
- Correlate security events across multiple telemetry sources, including network, authentication, memory, disk and configuration data, to identify discrepancies caused by incomplete or manipulated logs.
- Review trusted connectivity and administrative relationships with third parties and connected environments to identify potential pathways that could be leveraged for lateral movement.

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

Annex A - Indicators of Compromise

SHA1 Hash	Description
C164BFC953C66E58B11FC280E69FD43B8F255839	Custom SSH backdoor
1aa6ab2006b5d9199aa87bb0bbd995aec698ac4f	Custom SSH backdoor
c164bfc953c66e58b11fc280e69fd43b8f255839	Medusa rootkit binary
36005f5e4398a1c62a2a9271eddfcc1b44b1ad00	TacTap -Injector targeting tac_plus; injects /lib/libseconfd.so and listens on /var/run/acpid.lock
955cd45a2f6f226a2fdf44b329af1c8dde90cb38	TacTap – Injected TACACS library loaded into tac_plus; intercepts accepted TACACS sessions and sends descriptors to /var/run/acpid.lock.
13f0c2a598e3aa63856c032a96b110aed963f0e8	VMCI/VSOCK-based backdoor providing shell access through virtualization-adjacent channel
5ba1242050b5b447052b210788a5a25593d6987d	REPTILE like binary later renamed to masquerade as security agent processes.
7dab017f14628345d47bd4eb69cc49224f3054a7	Tinynshell
be6b27f429324a4af05a310d8ec9635e37c68a94	IOS XR implant
1682b652a15bde732489f22809b0b7594c228fd3	IOS XR implant
b149fa3a34bd585e7a674a4fd9538437bd06f514	IOS XR implant
6ef7d2985edf743ebff413a9298a127e9475d72f	Masqueraded startup script used for persistence

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Persistence	T1543.002	Create or Modify System Process: Systemd Service
	T1546	Event Triggered Execution
	T1098	Account Manipulation
Privilege Escalation	T1548	Abuse Elevation Control Mechanism
Defence Evasion	T1562.001	Impair Defenses: Disable or Modify Tools
	T1070.002	Indicator Removal: Clear Linux or Mac System Logs
	T1070.004	Indicator Removal: File Deletion
	T1036	Masquerading
Credential Access	T1056	Input Capture
	T1557	Adversary-in-the-Middle
Discovery	T1016	System Network Configuration Discovery
	T1049	System Network Connections Discovery
	T1046	Network Service Discovery
	T1087	Account Discovery
Collection	T1040	Network Sniffing
Command and Control	T1090	Proxy
	T1572	Protocol Tunnelling
	T1071.001	Application Layer Protocol: Web Protocols
	T1021.004	Remote Services: SSH
Exfiltration	T1048	Exfiltration Over Alternative Protocol

Annex C – Threat Hunting and Detection Opportunity

Asset class	High-signal hunting leads
Network devices	• Unexpected GRE or tunnel interfaces • Configuration state that differs from command output • PCAP generation from routers • FTP/SCP from routers • Command-accounting gaps • Shell access • Memory anomalies in legitimate network-device processes. • Traceroute or reachability testing to unusual external destinations
TACACS / AAA servers	• Tac_plus process injection • Credential-like artifacts under log or temporary directories • Command activity without corresponding login sessions • Unexplained encryption or xor-encoded files.
Linux jump hosts and management servers	• Selinux disabling • /var/tmp staging • /usr/lib/locate artifacts • Deleted-but-running processes • Custom SSH listeners • Suspicious iptables NAT or port redirection • Service names that imitate legitimate daemons or security agents.
Security-agent masquerading	• Unexpected binaries under security-agent directories • Security-agent-like processes that spawn shells, Python, scp, or network tools • Timestomped files matching nearby legitimate agent timestamps
Tunneling and scanning activity	• Repeated /var/log/secure entries containing sshd: error: connect_to ... port ... failed • Linux hosts with GRE tunnel configuration that are not approved network devices
Linux log and login-record tampering	• Use of utmpdump against /var/log/wtmp, /var/log/utmp, or /var/log/btmp • sed replacement of IP addresses inside login-history artifacts • sed -i '/sudo/d' against /var/log/*

References

1. ^ “Fire Ant Evolves: From Hypervisors to Trusted Infrastructure” 