# Magic Packet Malware Targeting Juniper VPN Gateways

## Overview

A sophisticated attack campaign (discovered by Lumen Technologie's Black Lotus Labs team) has targeted Juniper edge devices, including VPN gateways, using a malware variant called J-magic. This malware leverages "magic packet" technology to initiate a reverse shell, providing attackers with undetected, long-term access.

J-magic is a stealthy variant of the cd00r backdoor that targets Juniper devices and is designed for long-term access and minimal detection. It monitors traffic for a "magic packet" that meets specific conditions and opens a reverse shell for attackers who pass an RSA-encrypted challenge.

Operating entirely in memory, it evades detection and persists until the device is rebooted. To blend in, it disguises itself as a legitimate system process and overwrites its command-line arguments, making it difficult to identify.

**Affected Devices**

- Targeted Hardware - Juniper enterprise-grade routers and VPN gateways running Junos OS.
- Device Use - Perimeter and VPN gateway devices that lack host-based monitoring tools.

Failure to address this threat could result in unauthorized network access and long-term exposure.

## Aspire Protects

- Review hunt guides focused on BPF-based malware:
  - TrustedSec's blog on memory injection
  - SandFly Security blog
  - Elastic's blog with OSquery syntax
- Refer to this detection blog for cd00r malware for additional insights.
- Perform the following environment checks:
  - Search for all IoCs.
  - Review network logs for indicators of data exfiltration and lateral movement.

- Check for common persistence mechanisms on affected devices.

**TTPs to Watch**

Command and Control, Ingress Tool Transfer [T1105]

- The attacker establishes persistent access using a reverse shell initiated by the malware.

Defense Evasion, Obfuscated Files or Information [T1027]

- The malware uses command-line argument overwriting and masquerades as a legitimate process.

Execution, Exploitation for Client Execution [T1203]

- The initial infection vector remains unknown but may involve exploiting vulnerabilities or misconfigurations.

**IoCs**

MD5

- 4ca4f582418b2cc0626700511a6315c0
- d02283becb1376b1637a849ba2f159bd

SHA1

- 0ea36676bd7169bcbf432f721c4edb5fde0a46a9
- 7edc911b31b4f5dc401725c9b52e876a9fd00f3e
- bf3c1fc73fc20ed0ab2af3f1c81f5df7bdb3e4e8

SHA256

- 3f26a13f023ad0dcd7f2aa4e7771bba74910ee227b4b36ff72edc5f07336f115
- 5e3c128749f7ae4616a4620e0b53c0e5381724a790bba8314acb502ce7334df2
- 957c0c135b50d1c209840ec7ead60912a5ccefd2873bf5722cb85354cea4eb37
- c7cf51499973908cbc4c746f689b6ed245b26b1a9eae62fe9329f3a1036e82f4

For a complete list of IoCs associated with this attack campaign, please see Black Lotus Labs' GitHub page.

### Targeted Industries

Organizations in the semiconductor, energy, manufacturing, and IT sectors have been primary targets for this campaign.

## Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

## Supporting Documentation

The J-Magic Show: Magic Packets and Where to find them - Lumen Blog

IOCs/Jmagic_IOCs.txt at main · blacklotuslabs/IOCs · GitHub