THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

FamousSparrow

Threat Actor APT Group

Description

FamousSparrow

CATEGORY

APT Group

SEVERITY

High

Platforms

Windows

IMPACT

- Data Theft and Espionage
- Financial Losses
- Inhibit System Recovery

The FamousSparrow APT group, active since at least 2019 and previously thought dormant after 2022, has resurfaced with advanced variants of its custom backdoor SparrowDoor. Recent investigations uncovered ongoing cyber-espionage activity, including attacks on a U.S.-based financial trade organization, a government entity in Honduras, and a research institute in Mexico.

FamousSparrow is known for leveraging vulnerabilities in Microsoft Exchange, SharePoint, and Oracle Opera, including the high-profile ProxyLogon exploit chain. Their operations are characterized by stealth, long-term persistence, and the use of sophisticated malware.

THREAT OVERVIEW

SparrowDoor Backdoor

- Connects to a C2 server and exfiltrates host data: username, IP address, computer name, RDP session info.
- Accepts commands for lateral movement, file operations, reconnaissance, and credential harvesting.

ProxyLogon Exploit Chain

- Includes CVE-2021-26855, 26857, 26858, 27065
- Allows unauthenticated remote code execution on Microsoft Exchange Servers

Toolset Used

- **SparrowDoor** (custom backdoor)
- **ShadowPad** (modular espionage platform)
- **Mimikatz (modified)** – Credential theft
- **ProcDump** – Extracts LSASS memory
- **Nbtscan** – Scans for NetBIOS systems
- **Webshells** – Dropped via vulnerable IIS/Exchange configurations

Indicator of Compromise

MD5

8037d1d022ccc182d75b12b1c533df7d
54b419c2cac1a08605936e016d460697

SHA-1

C26F04790C6FB7950D89AB1B08207ACE01EFB536
1B06E877C2C12D74336E7532BC0ECF761E5FA5D4

SHA-256

d057034675befc1b4c2ae4132c4d169201c9abfbae79181185d45ca6721e43cc
d53346b5c8c6c76e7bc0407410a58328a1e214a4d359e558380963d29a35f71b

IPs

43.254.216.195
45.131.179.24
103.85.25.166
216.238.106.150

Remediation

Strategic

- Maintain regular threat intelligence ingestion and SOC briefing processes.
- Implement a proactive incident response framework focused on APT behavior.

Technical

- Patch all vulnerable Microsoft services (Exchange, IIS, and SharePoint).
- Monitor for:
  - Webshells on IIS
  - LSASS memory dumps
  - Suspicious outbound connections
- Use endpoint detection solutions capable of behavioral analysis.

Operational

- Initiate threat hunts for SparrowDoor-related IOCs and TTPs.
- Limit lateral movement via segmentation and least privilege principles.
- Investigate unrecognized RDP sessions and IIS process anomalies.

- Conduct regular **security awareness training** to build a security-conscious workforce.

Tactical Actions

- Apply the latest security patches and software updates across all systems and applications.
- Monitor and block known IOCs at network, endpoint, and perimeter levels.

ThreatCure

Cyber Threat Advisory

Secure your byte world

FamousSparrow

Threat Actor APT Group