THE FORENSICS WAY

ISSUE 02 | FORENSICS AWARENESS THIS WEEK | TUESDAY, FEBRUARY 3, 2026

FRONT PAGE

THREAT ACTOR SPOTLIGHT

The Lynx in the Network: Deconstructing RDP Infiltration

New forensic analysis reveals the predatory precision of **Lynx Ransomware**, a threat group increasingly leveraging exposed RDP credentials to secure initial access. Unlike louder counterparts, Lynx operators exhibit a "feline stealth," conducting extensive internal reconnaissance before deploying encryption payloads.

Analysts highlight that the group's methodology focuses on compromising domain controllers within hours of access, making rapid incident response critical for modern security teams.

FORENSIC METHODOLOGY

Evasion as an Art Form: How Lynx Bypasses Modern EDR

A deep dive into recent Lynx campaigns shows a sophisticated use of "Living-off-the-Land" binaries (LoLBins) to evade detection. By utilizing signed system tools for lateral movement and persistence, the group successfully blinds standard Endpoint Detection and Response (EDR) solutions.

Forensic examiners are urged to look beyond standard malware signatures and focus on behavioral artifacts in the Master File Table (MFT) and Windows Event Logs to identify Lynx's presence.

Threat Bulletin

CRITICAL

CVE-2026-4411

Remote Desktop Services Arbitrary File Execution. This flaw is actively being exploited by Lynx operators to drop initial stage loaders.

ACTIVE EXPLOIT

CVE-2026-5522

Windows Service Persistence Vulnerability. Allows attackers to maintain elevated access without triggering system integrity alarms.

MALWARE SPOTLIGHT

Lynx Ransomware

A sophisticated C++ based strain that prioritizes the destruction of shadow copies and the encryption of network shares via compromised administrative tokens.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, FEBRUARY 3, 2026

CASE STUDIES: HISTORICAL GRID

CASE STUDY: LYNX RANSOMWARE

The RDP Pivot Point

In a recent forensic engagement, Lynx operators gained access via a single non-MFA RDP account. Within six hours, they had mapped the entire network using legitimate tools, demonstrating the speed of modern ransomware pivots.

ARTIFACT ANALYSIS: LYNX

Persistence and Evasion

Detailed investigation into the Lynx execution chain reveals the use of custom scripts to disable security software prior to the deployment of the encryption engine, highlighting a need for immutable logging.

US V. BROWN (2025)

Landmark Biometric Ruling

Landmark D.C. Circuit ruling on biometric unlocking. This case addressed the Fifth Amendment implications of compelled biometric access to encrypted mobile devices.

CLOUD FORENSICS 2026

Encrypted RAM Snapshots

Impact of encrypted RAM snapshots on AWS. Investigators are now navigating a landscape where hypervisor-level encryption renders traditional memory dumping techniques obsolete.

PRIORITY CVE ADVISORIES

ARCHIVE ALERT

CVE-2026-21804 (APPLE)

Kernel-level memory corruption. Forensic Note: Monitor for unusual kernel extensions or unexpected system reboots.

ARCHIVE ALERT

CVE-2026-21990 (WINDOWS)

Print Spooler Local Privilege Escalation. Forensic Note: Check for spooler service restarts and unauthorized .dll writes in System32.

RECENT MALWARE WATCH

HISTORICAL CONTEXT

GOLDPICKAXE TROJAN

Sophisticated Trojan known for harvesting biometric face data. Examiners should look for unusual API calls to device camera modules.

SECTOR WATCH

SECTOPRAT V.2

Remote Access Trojan using "ClickFix" lures. Highly effective at credential exfiltration during the Lynx initial access phase.