Windows Artifact Forensics Lab. Prefetch, Shortcuts, and Jump Lists to Prove PlagueRat Use

Overview

In this lab, I performed endpoint triage using Windows user activity artifacts to reconstruct what a user accessed, what executed, and what browser activity occurred. The objective was to validate PlagueRat related activity using independent artifact sources, then stitch the evidence into a defensible activity timeline.

SOC handoff summary

Classification: Suspicious script and batch execution with supporting user activity artifacts
Severity: High
Confidence: High
Core artifacts: Shortcuts, Prefetch, Jump Lists
Key findings: User level access to PlagueRat content, confirmed execution artifacts tied to PlagueRat.bat, and supporting browsing evidence tied to Microsoft Edge

Tools used

Windows File Analyzer for shortcut analysis
PECmd.exe for Prefetch parsing and keyword searches
JumpListExplorer.exe for Jump List parsing
PowerShell for running tools and filtering output

Evidence sources and what they prove

Shortcuts. Evidence of files the user accessed and launched, plus file paths and access context
Prefetch. Evidence of program execution and related file references in execution context
Jump Lists. Evidence of recent items and browsing activity tied to a specific browser application

Investigation workflow and results

1. Triage and scope
   I focused on artifacts that provide high confidence user activity and execution proof. I used Shortcuts to identify what the user accessed first, Prefetch to validate what executed, and Jump Lists to validate related browsing behavior.

2. Shortcut evidence. What was accessed
   I analyzed the user Shortcuts location and identified PlagueRat related content and associated files that served as pivot points for the rest of the investigation.

Key shortcut artifacts extracted

- PlagueRat.ps1
- 2020_Summer_Photos.zip
- Invoice537 PR 06 05 2020.docx

Why this matters
Shortcuts provide a fast starting point. They establish the initial set of user touched artifacts to validate with execution focused evidence.

3. Prefetch evidence. What executed and what it touched
   I parsed Prefetch data to confirm execution context and identify the batch payload location tied to PlagueRat activity. I then used keyword based Prefetch searching to determine which applications interacted with the PlagueRat script.

Key Prefetch artifacts extracted
Batch payload confirmed
• PlagueRat.bat
• \USERS\IEUSER\PICTURES\SAVED PICTURES\2020_SUMMER_PHOTOS\2020 SUMMER PHOTOS\PLAGUERAT.BAT

Applications that opened PlagueRat.ps1
• notepad.exe
• powershell.exe

Why this matters
Prefetch provides strong execution evidence. It also helps connect user activity to execution and tooling used, which supports scoping and response decisions.

4. Jump List evidence. What site was visited and with what browser
   I loaded Automatic Destinations Jump List data and validated browser activity tied to a specific domain, then mapped it to the browser application used.

Key Jump List artifacts extracted
Visited domain
• https://discordapp.com
Browser used
• Microsoft Edge

Outcome and determination
The system contained multiple PlagueRat related artifacts across independent evidence sources. Shortcuts confirmed user level access to PlagueRat related content and related files. Prefetch confirmed execution context, revealed the batch payload path, and showed the PlagueRat script was opened using Notepad and PowerShell. Jump List analysis confirmed a visited domain and mapped that activity to Microsoft Edge. Based on the corroboration across artifacts, this should be treated as a confirmed suspicious activity chain pending broader scope validation.

Recommended response actions, production safe guidance

Immediate actions

- Preserve evidence, collect relevant artifacts and logs for the time window, and avoid altering timestamps
- Isolate the endpoint if this is a live case and suspicious execution is still in scope

Scoping actions

- Hunt across endpoints for PlagueRat.ps1 and PlagueRat.bat, including the specific user path observed
- Hunt for Prefetch entries and shortcut artifacts tied to the same filenames
- Review additional user activity artifacts for follow on execution, persistence, or lateral movement attempts if telemetry is available

Detection improvements

- Alert on PowerShell and Notepad opening suspicious script names in user writable directories
- Alert on execution of scripts and batch files from user profile picture and roaming style locations, especially when paired with suspicious shortcut evidence

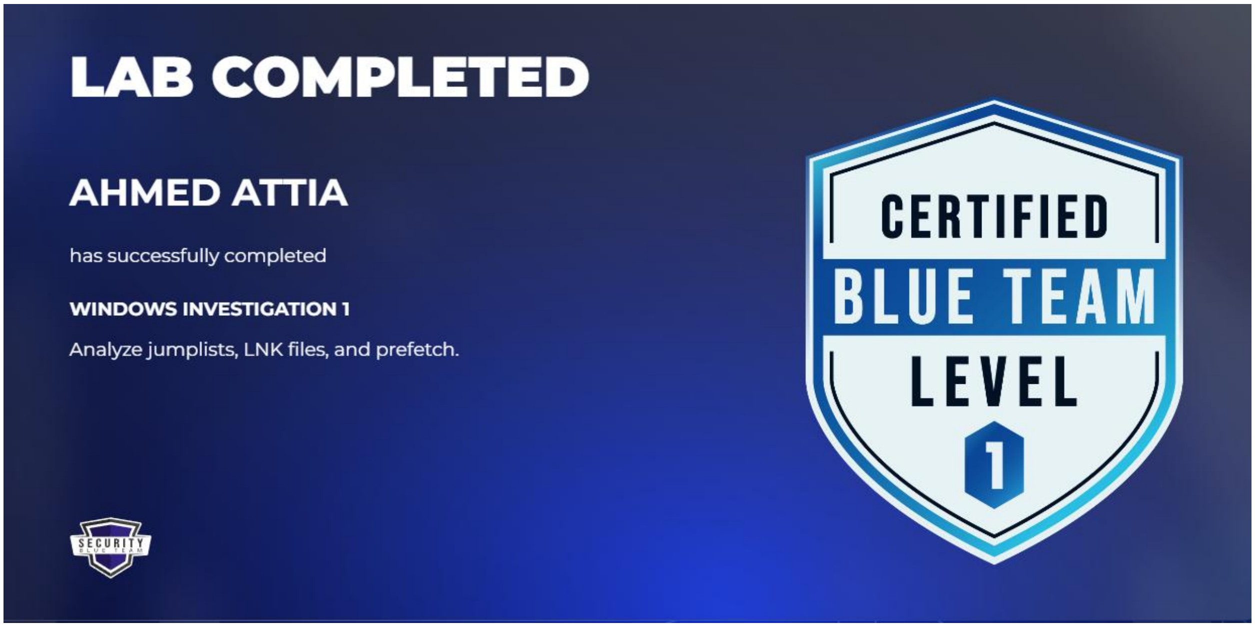
Skills demonstrated

Windows endpoint triage using multiple artifact sources

Evidence based timeline reconstruction using Shortcuts, Prefetch, and Jump Lists

Execution validation and scoping using Prefetch parsing and keyword searches

Clear, case style reporting that supports SOC handoff and escalation



LAB COMPLETED

AHMED ATTIA

has successfully completed

WINDOWS INVESTIGATION 1

Analyze jumplists, LNK files, and prefetch.

CERTIFIED
BLUE TEAM
LEVEL
1