Threat Analysis

@srozb - Sławek Rozbicki

TLP: Clear

Jul 17, 2025

What's Inside

Skeleton Spider/FIN6's delivery and execution chain dissected. Analysis of **100+ malicious LNK samples** from active campaigns targeting HR departments maps the complete attack flow—from initial ZIP delivery through LOLBin abuse to more_eggs backdoor deployment.

This technical deep-dive reveals consistent patterns across the entire execution chain: shared forensic metadata in LNK files, identical behavioral sequences for defense evasion, and predictable persistence mechanisms. Analysis of these patterns yields **actionable detection logic, targeted threat hunting opportunities, and actor tracking methodologies**.

Key intelligence includes:

- Complete delivery-to-execution chain analysis with forensic artifact mapping
- Pattern-based detection models targeting consistent LNK metadata and behavioral sequences
- Threat hunting opportunities leveraging shared creation timestamps and unique identifiers
- Actor tracking insights through infrastructure fingerprinting and campaign clustering techniques

Bottom line: While FIN6 continuously evolves their delivery infrastructure, their operational VM fingerprints remain embedded in forensic metadata. This research demonstrates how a single timestamp can transform 14+ months of seemingly scattered attacks into a trackable, huntable campaign pattern.

Background

FIN6/Skeleton Spider

Skeleton Spider, also known as FIN6, is a financially motivated cybercrime group that has evolved from point-of-sale breaches to broader enterprise threats, including ransomware operations. The group has demonstrated consistent adaptability in tactics while maintaining technical proficiency across multiple attack vectors.

Strategic Shift to HR Targeting

FIN6's most significant tactical evolution involves targeting human resources departments and recruitment professionals through sophisticated social engineering campaigns. The group leverages professional trust relationships by posing as job seekers, initiating contact through LinkedIn and Indeed to build rapport before delivering malicious payloads. This approach differs from earlier campaigns where actors posed as fake recruiters—now positioning themselves as fake job applicants to exploit the natural workflow of recruitment processes.

Prior Research Context

DomainTools **(June 2025)** documented FIN6's infrastructure modernization, specifically their adoption of AWS services to host convincing fake resume portfolios with traffic filtering mechanisms designed to evade automated security analysis. **Trend Micro MDR** **(September 2024)** provided tactical-level analysis following their successful mitigation of a more_eggs infection, mapping the complete attack chain from spear-phishing through persistence establishment using the Golden Chickens malware-as-a-service toolkit.

Current Activity

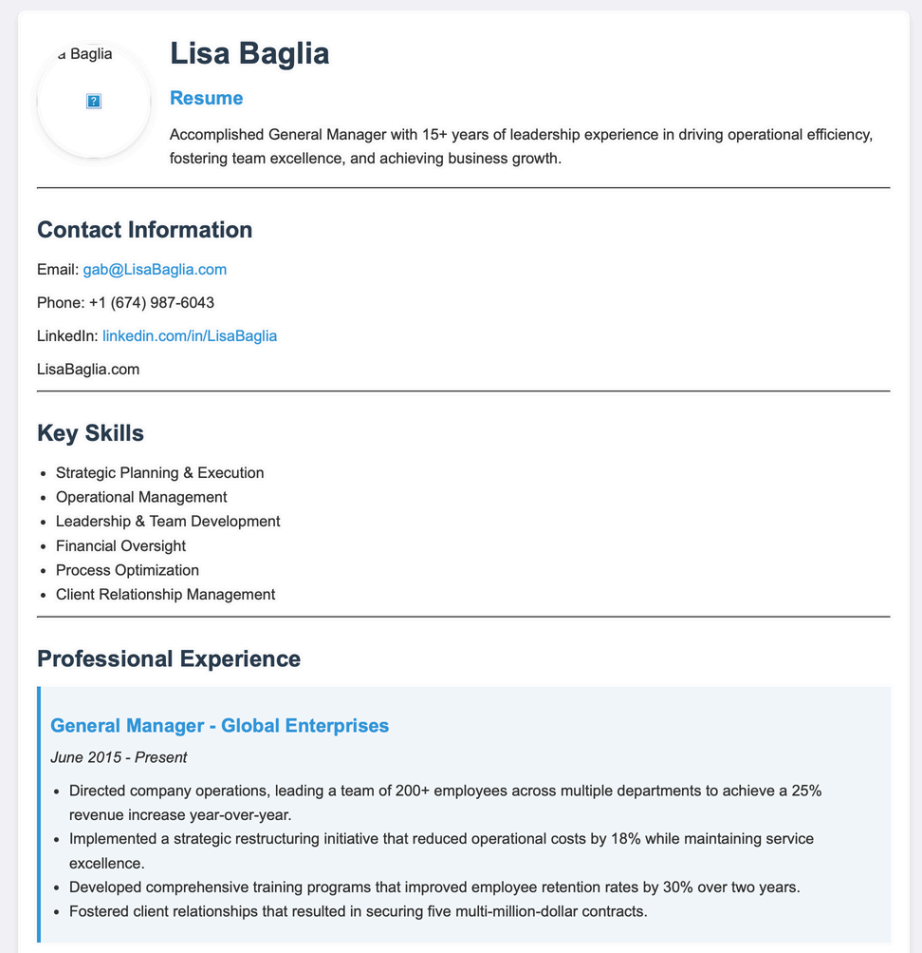
FIN6 remains operationally active with demonstrated consistency in toolset selection and technical implementation. Analysis of samples through July 2025 reveals continued reliance on weaponized LNK files, LOLBin abuse techniques, and registry-based persistence mechanisms, positioning the group as a persistent threat to organizations with active recruitment operations.

Delivery Sites Intelligence

Proactive infrastructure hunting revealed FIN6's template reuse and domain aging tactics. Censys-based reconnaissance uncovered two previously undetected delivery sites hosting identical fake resumes with shared contact details—same phone number (+1 674-987-6043), email pattern (gab@[domain].com), and professional experience templates. Both domains leverage aged registration histories, likely compromised or purchased legitimate sites now redirected to AWS infrastructure for reputation abuse. Historical analysis of one domain confirmed **it previously operated as a functioning business with active payment processing, validating this reputation abuse strategy.**

TLS certificate deployment indicates infrastructure activation since mid-June 2025, yet telemetry suggests limited operational usage—pointing to selective, targeted deployment rather than mass campaign activity. The sites exhibit rendering issues due to incomplete asset deployment, suggesting infrastructure still in development phases rather than active campaign use. This infrastructure pattern indicates FIN6's systematic approach to pre-staging delivery mechanisms well in advance of operational use, maintaining low detection profiles through domain aging and minimal pre-campaign activity while building the technical foundation for future targeted operations.

Hunting Note: Similar infrastructure can be identified through targeted Censys queries focusing on consistent content patterns and AWS hosting configurations associated with this campaign.



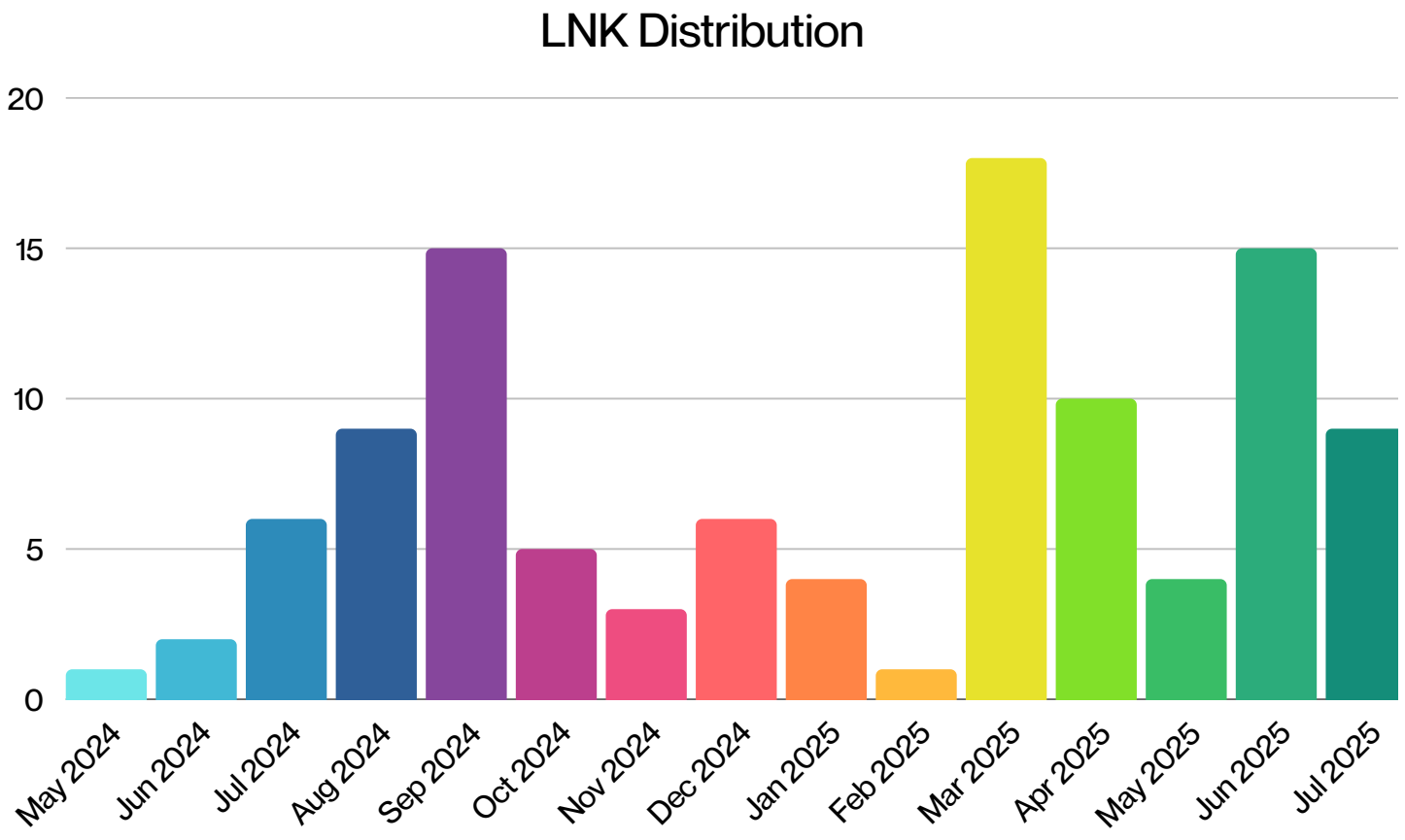
LNK Forensic Fingerprinting: The CreationTime Pivot

A single timestamp can unravel an entire campaign. While FIN6 cleverly tricks victims into manually typing URLs to sidestep link detection, the real intelligence lies within the LNK files' forensic metadata—details that remain invisible to users browsing shortcut properties in Windows.

Every malicious shortcut is carefully crafted to appear legitimate while hiding its true purpose from casual inspection, but here's where it gets interesting. They all share an identical **CreationTime** field of `2024-05-16T05:57:35.249121Z` with 100-nanoseconds (forensic) precision. This timestamp most likely represents when `cmd.exe` was created on the threat actor's operational VM, not the LNK file itself—effectively fingerprinting their attack infrastructure.

Using YARA's LNK module capabilities, security teams can pivot on this **CreationTime** to retroactively hunt across the entire sample set, regardless of how many times attackers change file hashes or obfuscation techniques. This creates a persistent signature that survives infrastructure rotation and file modifications.

The evidence is compelling: Analysis of 108 unique samples spanning May 17, 2024 through July 9, 2025 reveals sustained activity over 14+ months. While FIN6 constantly rotates their infrastructure—new domains, fresh IPs, different hosting providers—their underlying delivery mechanics remain surprisingly consistent. This metadata signature transforms what initially appears to be scattered, isolated attacks into a trackable campaign with measurable patterns, giving defenders visibility into the group's long-term operational habits.



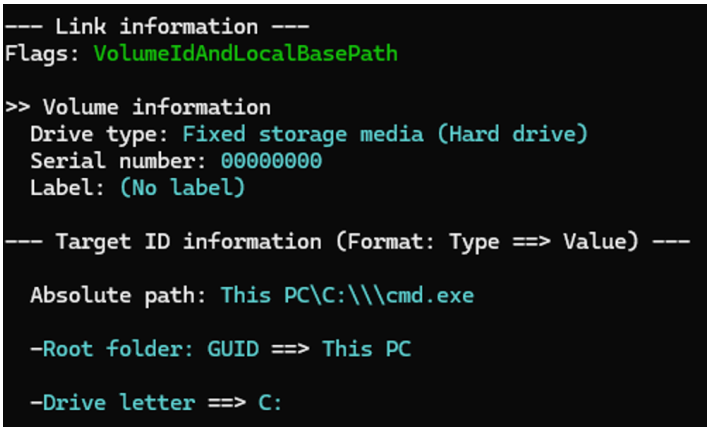
Payload Execution: Consistent LOLBin Abuse Patterns

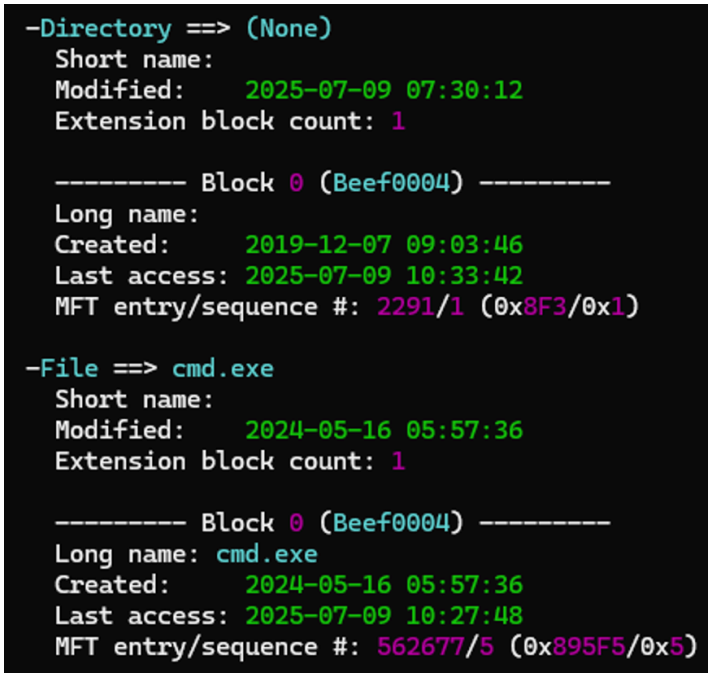
Technical execution remains remarkably consistent across 108 samples, confirming FIN6's standardized delivery methodology. The ZIP archives consistently contain a decoy JPEG file and the weaponized LNK file, which leverages legitimate Windows shortcut mechanisms in a sophisticated way. The LNK file targets `cmd.exe` using legitimate but poorly documented Windows shortcut resolution mechanisms, but hides its malicious payload entirely within the command line arguments—while the shortcut icon and properties still reveal `cmd.exe` as the target, the actual malicious command line remains hidden from Windows shell properties.

The payload behavior aligns perfectly with previous FIN6 research. All samples employ multi-phase variable substitution obfuscation to construct commands that copy the legitimate `ie4uinit.exe` LOLBin from Windows system directories to `%PUBLIC%` or `%TEMP%`, accompanied by a crafted `ieuinit.inf` configuration file. This combination downloads and executes the more_eggs backdoor component, following the exact execution chain documented in prior publications.

This sustained technical consistency validates FIN6's operational efficiency. The group has mastered concealing malicious behavior within legitimate Windows mechanisms, explaining their continued reliance on these LOLBin techniques despite infrastructure rotation. This approach achieves dual objectives: maintaining social engineering effectiveness while evading automated detection systems.

Parsed Shell Link Elements





Detection Opportunities: Consistent Patterns

Comprehensive deobfuscation of all 108 samples exposes reliable detection signatures across FIN6's execution methodology. Static analysis reveals universal reliance on `ie4uinit.exe` as the chosen LOLBin for payload download and execution, with identical deployment patterns that create multiple detection opportunities throughout the attack chain.

Consistent File Operations

All samples employ xcopy with identical switches for LOLBin deployment:

```
xcopy /Y /C /Q %windir%\system32\ie4uinit.exe [destination]
```

The sideloading directories follow a predictable pattern across five locations:

- `%APPDATA%\Adobe`
- `%APPDATA%\Microsoft`
- `%TEMP%`
- `%PUBLIC%`
- `%LOCALAPPDATA%\Temp\`

Execution Pattern Variations

Despite tactical variations in execution methods, all samples target `ie4uinit.exe` with the `-basesettings` argument:

- `powershell -Command "Start-Process '[path]\ie4uinit.exe' -ArgumentList '-baseSettings'"`
- `start %temp%\ie4uinit.exe -basesettings`
- `start /b /min %LOCALAPPDATA%\ie4uinit.exe -basesettings`
- `cmd /c %public%\ie4uinit.exe -basesettings`
- `wmic process call create "%appdata%\microsoft\ie4uinit.exe -basesettings"`

This consistency enables high-confidence detection across multiple vectors:

File System Monitoring: `ie4uinit.exe` copied outside `%WINDIR%\System32\` with accompanying ieuinit.inf creation in non-standard locations.

Process Execution: `ie4uinit.exe` execution from non-system directories with `-basesettings` parameter, regardless of parent process variation.

Command Line Pattern Matching: Universal xcopy switches (`/Y /C /Q`) targeting `ie4uinit.exe` provide reliable behavioral signatures.

Research Transparency

All investigated LNK files, extracted and deobfuscated payloads, along with the analysis tools developed for this research, are available in the public repository: **https://github.com/srozb/less_eggs**

IoC

YARA rule

```
import "lnk"


rule lnk_hr_campaign {
  meta:
    description = "FIN6 weaponized lnk targeting recruiters & hr"
    author = "Sławek Rozbicki (@srozb)"
    sample = "ffc1262ead44f91f4d283d66d599b3d3277368ef4dd1cde6cb078ce0a1d90016"
    creation_date = "2025-07-16"
    last_modified = "2025-07-16"
    version = "1.0"
    sharing = "TLP:CLEAR"
condition:
    lnk.is_lnk and (
      lnk.creation_time == 1715839055 or
      lnk.tracker_data.droid_volume_id == "0b7699cc-2521-4ea7-98eb-a4b2d47d21d0" or
      lnk.tracker_data.droid_file_id == "1edf70a0-137a-11ef-a4fb-00155da53e0d" or
      lnk.tracker_data.droid_birth_volume_id == "0b7699cc-2521-4ea7-98eb-a4b2d47d21d0" or
      lnk.tracker_data.droid_birth_file_id == "1edf70a0-137a-11ef-a4fb-00155da53e0d"
    )
  }
```

Sigma Rules

d3bf399f-b0cf-4250-8bb4-dfc192ab81dc: Ie4uinit Lolbin Use From Invalid Path

9e50a8b3-dd05-4eb8-9153-bdb6b79d50b0: Msxsl.EXE Execution

fff9d2b7-e11c-4a69-93d3-40ef66189767: Suspicious Copy From or To System Directory

Domains

amaureira[.]com

bettystephen[.]com

bobbyweisman[.]com

brokarry[.]com

davidopkins[.]com

edwarddhall[.]com

emersonkelly[.]com

frankcossio[.]com

gabrielanielsen[.]com

garyscape[.]com

jacketman[.]net

jacksallay[.]com

johncboins[.]com

johnclawrence[.]com

julienolsson[.]com

katherinehutchens[.]com

kimberlykamara[.]com

lisabaglia[.]com

malenebutler[.]com

markqualman[.]com

michaeljacobs[.]info

mickigrimland[.]com

mikedecook[.]com

mitchellspearman[.]com

pasatasfn[.]com

pasdk[.]com

patrickbeltrame[.]com

paul-stein[.]com

sophia-pascal[.]com

teresamalins[.]com

SHA256

ebaa806ba4b40d7f89d93f6124edf4cd66a3f3a4f281081aa5eccc987c18d846

11a469ad6ae7b5e77d9824176cb69bbeed8bf3e7dbdd39b797249c4fbefc2163

dde548a4c9f7b039b6fd7921423096dbc30fc562dc32cad206362a166778be00

9495e0915feebbc641a1c127327889030ac5553f1731d8a375c2ed5b49214217

6e225615e0c90244e94d63d238459b03a018a058bbe59f5382b42cf414008393

a6d897cd814926fe0657f4946a66012ec969fd5ec31d5fb96095478113fb913e

64e0d9bd56374e1528e8f312b21b3f7add63feacf61ce9d4315b7d2578c3e1ef

13361d1b8dcf6e26e3f36a3435f748b4b5556ac581ecc2084b7ebff16dca5555

07a5beba5470734e8e465e89b7eee3d6f0672c47b63b33f9f6f56eccdc0c4755

7d05db7f4cbf2251b2708349b7edfe448af83ee5616116012a044ec810d32e5b

f115187143a80b062a4844dbd462ed183e374263eeea874780eb65775991da22