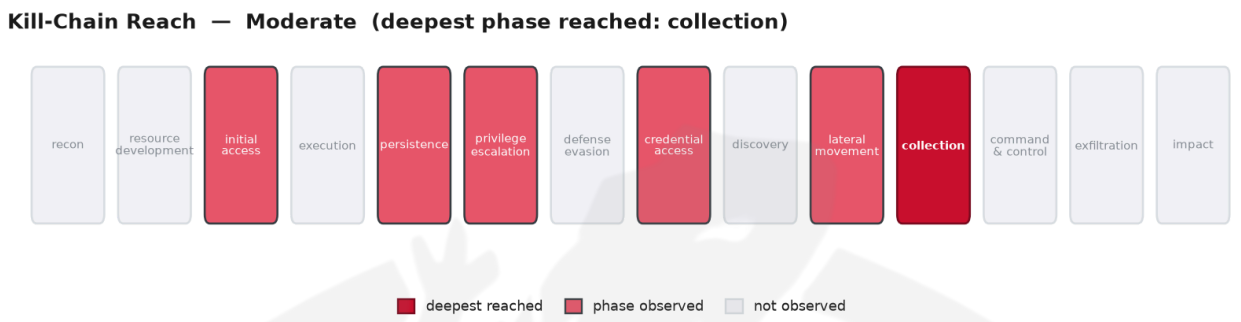
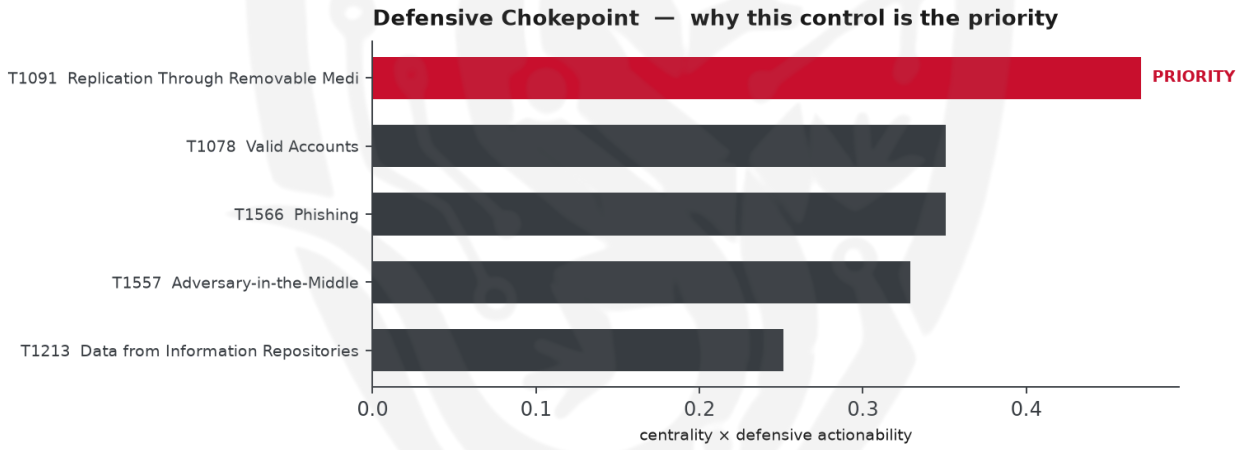
THREAT REPORT: UNC3753 TARGETS US LAW FIRMS

Visual Summary



How far down the attack chain this campaign reached; deepest phase in crimson.



The control that most disrupts the attack (priority in crimson).

Summary

The source attributes this activity to UNC3753, a threat actor targeting US law firms with various malware families, including LOCKBIT.BLACK, BAZARLOADER, and TrickBot. The targeted sectors include finance and government, with the threat actor likely seeking sensitive information. Priority should be given to defending against the replication of malware through removable media. The actor's use of multiple malware families and techniques poses a moderate operational risk.

Threat Overview

UNC3753, the attributed threat actor, is using a range of malware families, including LOCKBIT.BLACK, BAZARLOADER, and TrickBot, to target US law firms. The victimology suggests that the threat actor is interested in collecting sensitive information from the targeted sectors. The central vulnerability exploited is not specified due to insufficient data.

Attack Chain and Priority Control

The observed techniques, inferred from the report, include the use of valid accounts, replication through removable media, and phishing. The priority technique is T1091 Replication Through Removable Media, which is the graph chokepoint. The lead control is to Apply the specific MITRE ATT&CK mitigation for this technique; add host/network detections and least-privilege controls around it.

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this activity. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB confidence of 80% or higher, with the highest confidence seen being 0%.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, machine-extracted from report text — reduced confidence)

The source pulse carried no expert ATT&CK tags, so these techniques were inferred from its narrative by a self-consensus LLM extractor and validated against the ATT&CK catalogue. Treat this technique set, and the chokepoint, kill-chain and risk scores derived from it, as lower-confidence than an expert-tagged brief. - T1078 Valid Accounts - T1091 Replication Through Removable Media - T1213 Data from Information Repositories - T1557 Adversary-in-the-Middle - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1091 Replication Through Removable Media (centrality 0.47).
- Operational risk: Moderate (score 0.458, reaches collection).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3162; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

Historical Profile	Behavioural Overlap
AppleJeus	0.3162

Historical Profile	Behavioural Overlap
Sea Turtle	0.2828
PittyTiger	0.2582
APT30	0.2236
LuminousMoth	0.207

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator
Domain	business-data-leaks[.]com
Domain	lockbit[.]black
Domain	itdesk[.]com

Flame Cell // Adversary Pivot [BETA]

BETA. A hypothetical tabletop projection, anchored to documented ATT&CK behaviour and technique co-occurrence across 170 tracked groups. It is not a prediction; treat it as a war-game prompt and review before acting. Spot a pivot that looks wrong? norbert@salacti.com

- **Control applied:** T1091 Replication Through Removable Media (initial-access)
- **Observed here:** T1091 Replication Through Removable Media was the initial-access control point; blocking a means-of-entry rarely stops a determined actor, so the pivot projects forward to the execution stage they must still reach.
- **Projected pivot:** T1203 Exploitation for Client Execution (execution)
- **Basis:** of the 5+ groups that use Replication Through Removable Media, this pairing runs 2.6x above base rate, a disproportionately-coupled move rather than the obvious one.

The adversary, UNC3753, could pivot to T1203 Exploitation for Client Execution to maintain their objective by leveraging vulnerabilities in client applications, such as browsers or Office software, to execute malicious code on compromised hosts, potentially exploiting the trust users have in these applications. This technique may be particularly appealing as it allows the adversary to execute code without relying on removable media, which has been blocked. To counter this potential pivot, the mandated defensive control

of patching client applications, enabling exploit mitigations such as ASLR, DEP, and CFG, and implementing application isolation would likely be effective.

Also plausible (same tactic): T1559 Inter-Process Communication (n=3, lift 4.6), T1106 Native API (n=3, lift 3.2)

Detection and hardening for the pivot (T1203 Exploitation for Client Execution)

- **Telemetry:** EDR process + memory telemetry; Office/browser/reader child-process telemetry; Windows Error Reporting (application crashes)
- **Detect:**
  - Office, browser or PDF-reader processes (winword/excel/outlook/acrobat/chrome) spawning shells or LOLBINs
  - Sysmon 1 anomalous children of document/browser apps; unbacked-memory execution right after a client crash
  - WER application-crash events for client apps immediately followed by a new child process
- **Harden:**
  - Patch client software fast (browsers, Office, PDF, Java); retire end-of-life plugins
  - ASR rules blocking Office child processes; exploit protection (DEP/ASLR/CFG) and browser sandboxing
- **MITRE:** M1048 Application Isolation and Sandboxing, M1050 Exploit Protection, M1051 Update Software, M1040 Behavior Prevention on Endpoint · DS0009 Process, DS0011 Module, DS0015 Application Log