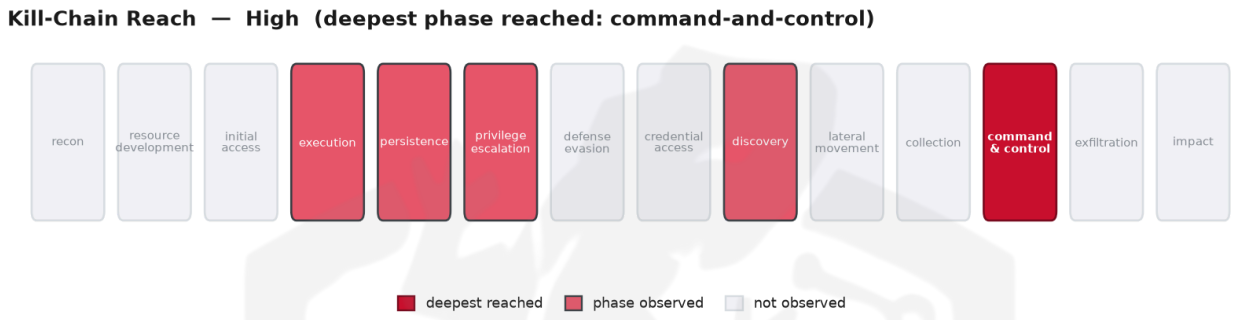
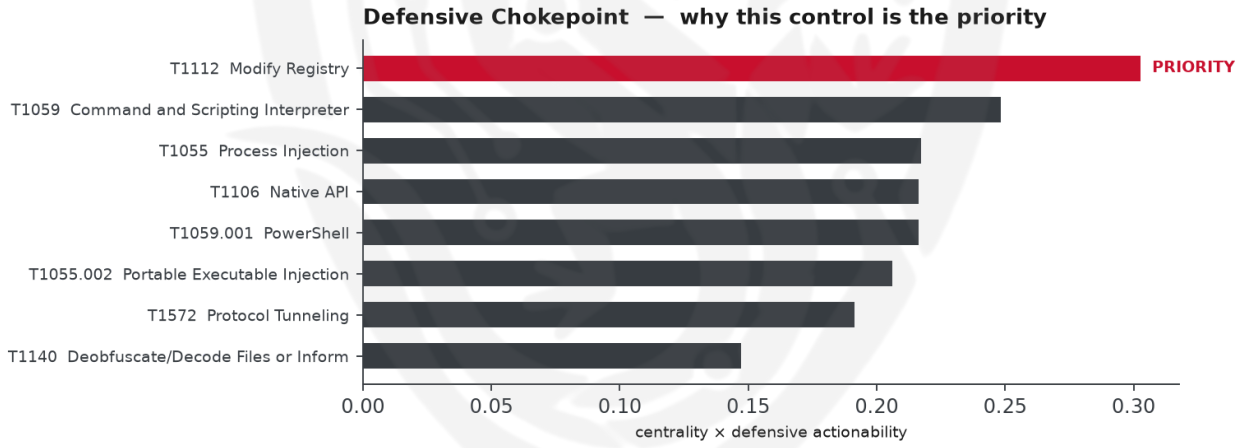
THREAT REPORT: TRICKBOT VARIANT UTILIZING DNS TUNNELING

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 observed cluster of activity involves a TrickBot variant that utilizes DNS tunneling for command and control. This malware targets unspecified sectors and countries, and its central vulnerability is currently unknown. Priority should be given to monitoring sensitive registry keys for modification to mitigate the threat. The threat actor's identity and specific targets remain unclear due to insufficient data.

Threat Overview

The threat actor, whose identity is not specified, is associated with the TrickBot malware family, including variants such as Totbrick and TSPY_TRICKLOAD. The malware exploits unspecified vulnerabilities and uses various techniques, including DNS tunneling, to achieve its goals. The victimology of this campaign is not well-defined due to a lack of information on targeted countries and sectors.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including scheduled tasks, system information discovery, and protocol tunneling, ultimately leading to command and control via DNS tunneling. The priority technique identified is T1112, Modify Registry, which serves as a critical chokepoint in the attack chain. To counter this, the priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs used by the threat actor, as indicated by the lack of data in the infrastructure and corroboration section. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB confidence level 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, expert-tagged by source)

- T1053.005 Scheduled Task
- T1218.011 Rundll32
- T1071.004 DNS
- T1497.001 System Checks
- T1082 System Information Discovery
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1572 Protocol Tunneling
- T1112 Modify Registry
- T1059 Command and Scripting Interpreter
- T1055.002 Portable Executable Injection
- T1059.001 PowerShell
- T1027 Obfuscated Files or Information
- T1012 Query Registry
- T1564.003 Hidden Window
- T1055.005 Thread Local Storage
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.3187).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4446; 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
Gorgon Group	0.4446
Gamaredon Group	0.4246
APT19	0.4146
Daggerfly	0.3892
FIN7	0.3537

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	westurn[.]in
Hash	8d5b3a0512744efc132afa6fc75c64d8
Hash	f7f2f482f3bc6345a44e4a6d647731ae
Hash	48fd2036b6556c6747197e07f1706bcf58a27518
Hash	105f652e6b8f31c371f2385877e43b6772aff5d3168d5d4635f8a1fcbb321421
Hash	33c331ededbf8ee9829895424423ce3fd17e359d2e784fcbce396aacff458cf5
Hash	3b19a82e1354ac14a3da7c840cbdd0ce50db38432d78e767b36f08e45024c23d
Hash	6c677eb2b3ffd288083c59a13d7bb712d4754af61a5563873f76c440962346f4
Hash	bf80245ba792992fbfe24abac33f8fd66f24cdeb5f0f21cfdf45a29d107c8d3b

Type	Indicator
Hash	df527a5c2fbde43816cd02f4cd49eee4bb82fb4a3c7045021360888c7d504c98

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:** T1112 Modify Registry (persistence)
- **Observed here:** T1112 Modify Registry was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1543 Create or Modify System Process (persistence)
- **Basis:** of the 14+ groups that use Modify Registry, this pairing runs 2.8x above base rate, a disproportionately-coupled move rather than the obvious one.

With T1112 Modify Registry blocked, the threat actor could preserve the same objective by pivoting to T1543 Create or Modify System Process, a technique disproportionately paired with it across tracked groups. Defensive countermeasure: Restrict service/daemon creation to admins; monitor service and driver installs.

Also plausible (same tactic): T1547 Boot or Logon Autostart Execution (n=17, lift 1.7), T1505 Server Software Component (n=11, lift 2.0)

Detection and hardening for the pivot (T1543 Create or Modify System Process)

- **Telemetry:** Windows Security / System log; Sysmon
- **Detect:**
  - System 7045 (new service installed); Security 4697 (service installed)
  - Sysmon 1 for sc.exe / services created; unusual ImagePath or user-context services
  - Registry writes under HKLM\SYSTEM\CurrentControlSet\Services
- **Harden:**
  - Restrict service creation to admins; application control on service binaries
  - Baseline installed services and alert on new/anomalous ones
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0019 Service, DS0024 Windows Registry, DS0009 Process