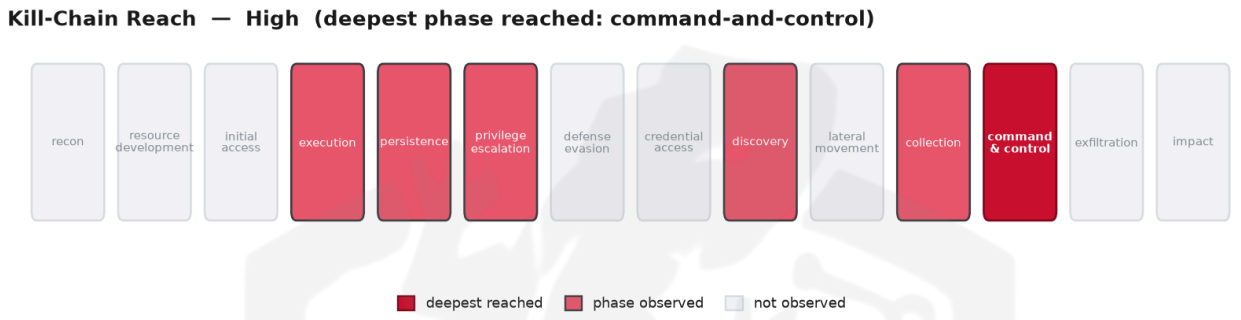
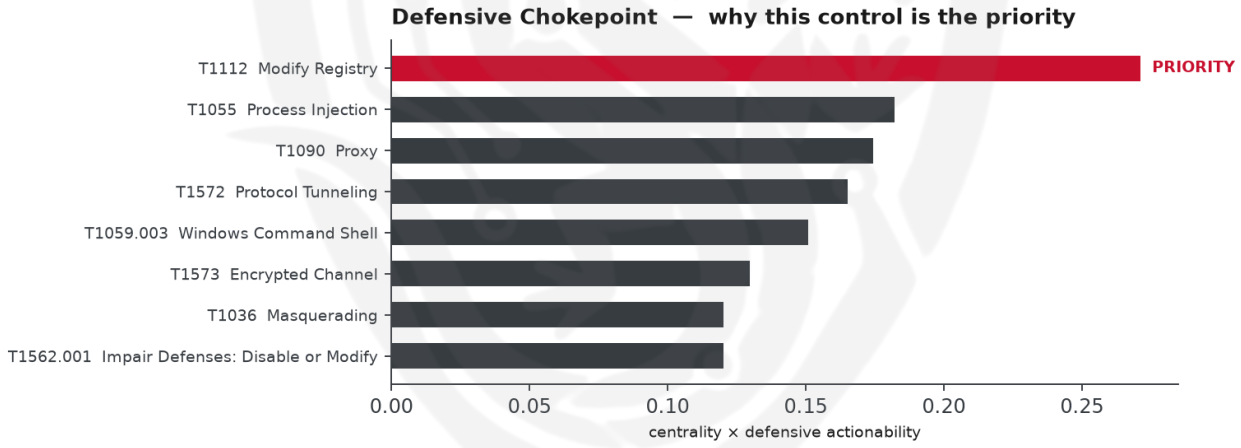
THREAT REPORT: UNKNOWN_ADVERSARY HELLONET CAMPAIGN

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 has been identified as the HelloNet campaign, which targets various sectors in the Russian Federation, including Government, Energy, Transportation, Education, and Aerospace. The campaign involves the use of multiple malware families, including HelloInjector, HelloProxy, HelloExecutor, HelloCleaner, and HelloBackdoor. Priority should be given to monitoring sensitive registry keys for modification to mitigate the threat. The threat actor's identity remains unknown due to insufficient data.

Threat Overview

The threat actor, referred to here as the observed cluster of activity, utilizes a range of malware families to compromise systems. The malware families involved are HelloInjector, HelloProxy, HelloExecutor,

HelloCleaner, and HelloBackdoor. The campaign targets organizations in the Russian Federation across multiple sectors. The exploited vulnerability is not specified due to insufficient data.

Attack Chain and Priority Control

The attack chain involves various techniques, including Local Data Staging, Windows Service, System Service Discovery, and others. The priority technique identified is T1112 Modify Registry, which serves as a critical point in the attack chain. To counter this, the recommended priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

The malicious infrastructure associated with this campaign is hosted by providers such as LLC Baxet and Newserverlife LLC. However, according to abuse.ch, there are no corroborated malware families. Additionally, AbuseIPDB does not flag any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%. These findings are based on third-party enrichment and serve to corroborate the source pulse without overriding it.

Technical Appendix

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

Observed Techniques (ATT&CK, expert-tagged by source)

- T1074.001 Local Data Staging
- T1543.003 Windows Service
- T1007 System Service Discovery
- T1082 System Information Discovery
- T1071 Application Layer Protocol
- T1005 Data from Local System
- T1036 Masquerading
- T1055 Process Injection
- T1572 Protocol Tunneling
- T1112 Modify Registry
- T1016 System Network Configuration Discovery
- T1090 Proxy
- T1083 File and Directory Discovery
- T1049 System Network Connections Discovery
- T1057 Process Discovery
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1573 Encrypted Channel
- T1059.003 Windows Command Shell
- T1070.004 File Deletion
- T1018 Remote System Discovery

- T1574.002 Hijack Execution Flow
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.2855).
- 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 0.4575; 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
APT3	0.4575
Tropic Trooper	0.4543
menuPass	0.3969
MirrorFace	0.3969
TeamTNT	0.3926

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	Context
IP	176[.]32[.]34[.]135	AS51659 LLC Baxet
IP	5[.]39[.]253[.]206	AS49791 Newserverlife LLC
Hash	0cfdffc56f0fa325d0c4d24780b46597	

Type	Indicator	Context
Hash	16c211c96735f2fae9361b89bd7a31bf	
Hash	1bfe2b9493128574907a8279256a8bcc	
Hash	41c938b3cd7e55d4077e34976929b140	
Hash	6001829a128fe264b4403138700c11a8	
Hash	9f5606a0755bc633b9bd7db6d179c09e	
Hash	b103cd21280b4061f88b2bcc51394894	
Hash	ee4ff46ddd8489e81447962f927bc3f6	
Hash	f9eed2f0158dc98e7012fb809152209c	
Hash	686292c07e33c4a5ca456db446bb71fb9fc67a81	
Hash	ffdc194775b2904564bbbd1cf0eb01d1a01f83ef5197d1612b6e2d69de7a4732	

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.

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:** the threat actor used T1543.003 Windows Service here as an alternative persistence technique.
- **Projected pivot:** T1543.003 Windows Service (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to utilizing Windows services, specifically creating a new service, to maintain persistence and evade detection, which may allow them to achieve their objective despite the registry

modification block. This technique, T1543.003 Windows Service, would likely involve creating a malicious service that blends in with legitimate system services. To counter this potential move, the defensive control of Restrict service/daemon creation to admins; monitor service and driver installs should be implemented.

Detection and hardening for the pivot (T1543.003 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