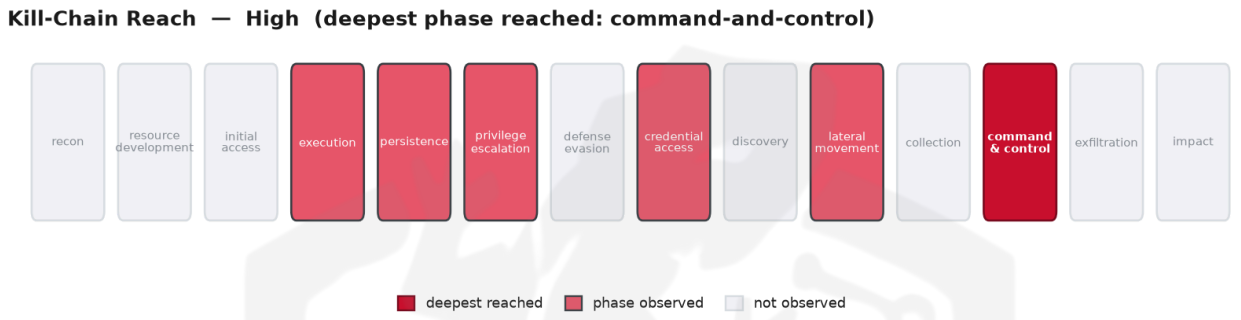
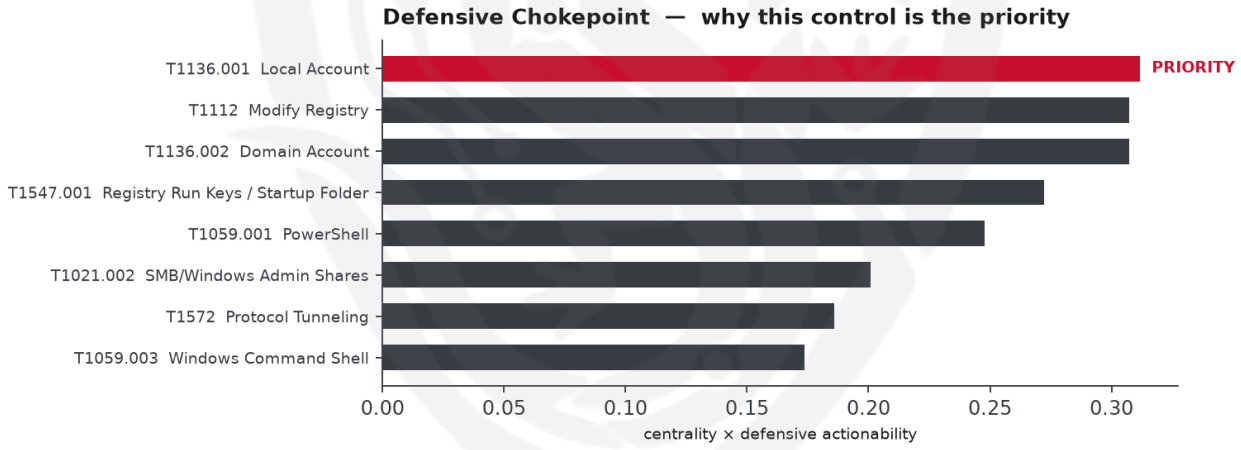
THREAT REPORT: THE GENTLEMEN AFFILIATE DEPLOYS ETHERRAT

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 Gentlemen threat actor has been observed deploying EtherRAT malware across Windows networks, utilizing an Ethereum smart contract as a command and control (C2) mechanism. The targeted countries and sectors are currently unknown. Priority should be given to monitoring and controlling the creation of new local and domain accounts, as this is a critical point in the attack chain. The Gentlemen's use of multiple malware families, including Sliver and Chisel, poses a significant threat to Windows networks.

Threat Overview

The Gentlemen threat actor is utilizing a range of malware families, including EtherRAT, Sliver, Chisel, Ligolo-ng, and Mimikatz, to compromise Windows networks. The central vulnerability exploited is currently unknown. The actor's use of Ethereum smart contracts as a C2 mechanism adds a layer of complexity to

the attack. The victimology of the attack is also unknown, with no specific countries or sectors identified as being targeted.

Attack Chain and Priority Control

The observed techniques used by The Gentlemen threat actor form a complex attack chain, involving the use of scheduled tasks, Windows Management Instrumentation, and JavaScript. However, the priority technique is the creation of new local accounts, identified as T1136.001. To mitigate this, the priority control is to alert on new local/domain account creation (Event ID 4720/4728) and enforce an approval workflow for account provisioning.

Infrastructure and Corroboration

The malicious infrastructure used by The Gentlemen threat actor is hosted on a range of providers, including NetCrafters OU, Cogent Communications LLC, Host Sailor Ltd, and Servers Tech Fzco. Abuse.ch has corroborated the use of EtherRAT and Sliver malware families, providing additional context to the attack. However, no indicators have been flagged with high confidence by AbuseIPDB, 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
- T1047 Windows Management Instrumentation
- T1059.007 JavaScript
- T1003.002 Security Account Manager
- T1218.007 Msiexec
- T1021.002 SMB/Windows Admin Shares
- T1572 Protocol Tunneling
- T1112 Modify Registry
- T1136.001 Local Account
- T1136.002 Domain Account
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1102.001 Dead Drop Resolver

Analytical Scores

- Priority technique (graph chokepoint): T1136.001 Local Account (centrality 0.3282).
- 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 0.45; 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
Rancor	0.45
Daggerfly	0.4382
BlackByte	0.4185
Wizard Spider	0.417
FIN13	0.4157

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: EtherRAT, Sliver.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
IP	193[.]233[.]202[.]17	AbuseIPDB 0% (US) · Sliver · AS203273 NetCrafters OU
IP	185[.]45[.]193[.]151	AbuseIPDB 0% (NL) · AS60117 Host Sailor Ltd
IP	38[.]110[.]228[.]43	AbuseIPDB 0% (US) · AS174 Cogent Communications LLC
IP	77[.]110[.]122[.]137	AbuseIPDB 0% (US) · AS203273 NetCrafters OU

Type	Indicator	Context
IP	77[.]110[.]126[.]46	AbuseIPDB 0% (US) · AS203273 NetCrafters OU
IP	77[.]110[.]122[.]58	AbuseIPDB 0% (US) · AS203273 NetCrafters OU
IP	146[.]103[.]127[.]44	AbuseIPDB 0% (NL) · AS216071 Servers Tech Fzco
IP	185[.]117[.]72[.]215	AbuseIPDB 0% (NL) · AS60117 Host Sailor Ltd
IP	38[.]110[.]228[.]125	AbuseIPDB 0% (US) · AS174 Cogent Communications LLC
IP	38[.]110[.]228[.]33	AbuseIPDB 0% (US) · AS174 Cogent Communications LLC
IP	50[.]114[.]167[.]112	AbuseIPDB 0% (US) · AS212238 DataCamp Limited
Domain	resumeacceptable[.]com	
Domain	publisherresolution[.]com	EtherRAT
Domain	simultaneouslypower[.]com	EtherRAT
Domain	wiselystarting[.]com	EtherRAT
Domain	itemrange[.]com	EtherRAT
URL	hxxp://193[.]233[.]202[.]17:9001	
Hash	4b690f3ce585df982a042917b82642c8	
Hash	bd1eaea733425cd21a51a652c429951d	Sliver
Hash	60285f6776cc3ff20872feeee7f2fd0b3b04410d	Sliver
Hash	9dd99bc68e60132f32fc33617deb9583c8cebb51	
Hash	73955566338adffb423c3b7608792963080da780e8b7b2c2cd6b6b0cef6f217f	

Type	Indicator	Context
Hash	7567994310a9576b1f98dc672ecfa038f1d65084315f59e3883f9b6f24000073	
Hash	756c2096f54c5497110c9d854625c3ed592873e566d532077cd7adb4d10d4add	
Hash	86881b8e9d197ac2f734792de48d5dfaebe7cafb6e35d49c5dd7fe6eb697230e	
Hash	bd61c2880920bbfb86c12df439dd1ca0258a10e532433698fd029aef2a5b33f2	Sliver
Hash	c7a80576fbd25057435652788591d13998da272edf627fc29d296684cefc50e5	
Hash	ee6807a8abfabced22ee026e178a28da64d13cc3408e224394ff6e5782fb9e1d	
Hash	f4c87a1df04274b7497cbf9a4619b946c915cf5210b6e2eaa2fee1629f4ff196	
Hash	f609621698eaad8c4683750fe8bd0e242349be3eea408da593151ff877ed8ab6	
Hash	f659681525debda69fe0865b2b27a42f684b1fda66aa7398e80b84cc765c73c7	
Hash	fb94688ed37dfcb985a8a4d720230e5150956e1788d579b0a54b53a153fd2f2e	

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:** T1136.001 Local Account (persistence)
- **Observed here:** T1136.001 Local Account was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1098 Account Manipulation (persistence)
- **Basis:** of the 13+ groups that use Local Account, this pairing runs 5.6x above base rate, a disproportionately-coupled move rather than the obvious one.

The Gentlemen could pivot to T1098 Account Manipulation in an attempt to maintain access and escalate privileges, as this technique would allow them to modify existing accounts to bypass the blocked local account creation, potentially by adding themselves to a high-privilege group or modifying a existing account's permissions. This technique may be particularly appealing as it leverages existing accounts, potentially reducing the noise generated by the attack. To counter this, the defensive control of alerting on privilege/group changes and credential additions to accounts (Event ID 4738/4670) and reviewing conditional-access changes should be implemented.

Also plausible (same tactic): T1505 Server Software Component (n=12, lift 2.9), T1133 External Remote Services (n=10, lift 2.8)

Detection and hardening for the pivot (T1098 Account Manipulation)

- **Telemetry:** Windows Security (account management); Azure AD audit logs
- **Detect:**
  - Security 4728/4732/4756 (added to security-enabled groups), 4738 (account changed), 4670 (permissions changed)
  - New credentials/keys added to accounts or app registrations in the IdP
  - MFA method added or reset outside a normal workflow
- **Harden:**
  - Alert on privileged-group changes; approval workflow for role grants
  - Monitor and restrict service-principal credential additions
- **MITRE:** M1032 Multi-factor Authentication, M1026 Privileged Account Management, M1018 User Account Management · DS0002 User Account, DS0026 Active Directory