



THREAT ADVISORY

Toy Ghouls Deploys Angry Birds Backdoor via MQTT and Element

PREPARED BY

Drona Cyber Solutions Pvt Ltd

DATE OF ISSUE

September 8, 2026

CLASSIFICATION MATRIX

TLP : GREEN

THREAT ADVISORY: TOY GHOULS DEPLOYS 'ANGRY BIRDS' BACKDOOR FRAMEWORK

Strategic Threat Intelligence Briefing on Emerging MQTT and Element/Matrix Command-and-Control Operations

THREAT ACTOR	Toy Ghouls	INFORMATION CLASSIFICATION	TLP: GREEN
KNOWN ALIASES	Bearlyfy, Laboo.booo, Feral Wolf	PUBLICATION DATE	September 08, 2026
MALWARE FRAMEWORK	'Angry Birds' (mqtt-bird-agent, matrix-bird-agent)	DELIVERY MECHANISM	Windows Remote Management (WinRM)
TARGET GEOGRAPHY	Russian Federation / Eastern Europe	ADVISORY URGENCY RATING	ELEVATED (PRIORITY ACTION)

1. EXECUTIVE SUMMARY

Drona Research and Intelligence Labs (DRIL), alongside enterprise cybersecurity intelligence feeds, has analyzed an advanced campaign orchestrated by the financially motivated threat actor known as TOY GHOULS (tracked under industry aliases BEARLYFY, LABOO.BOOO, and FERAL WOLF). Previously known for deploying commodity tooling and proprietary ransomware variants such as GenieLocker, Toy Ghouls has advanced its technical sophistication through the development and active deployment of custom-built implants.

The actor group has deployed a proprietary dual-variant backdoor suite internally designated as 'ANGRY BIRDS'. This framework introduces two distinct payload variants: mqtt-bird-agent (v0.1.0), which channels command-and-control (C2) operations through enterprise-grade HiveMQ MQTT message brokers over port 8883, and matrix-bird-agent (v0.1.0), which conducts covert operations through the decentralized Element messenger over the Matrix protocol. Both payloads are staged and propagated laterally using Windows Remote Management (WinRM) and persist natively as dedicated Windows background services.

To frustrate forensic response and automated sandbox detonation, both variants incorporate host-locked configuration encryption utilizing the ChaCha20-Poly1305 algorithm, cryptographically seeded by the target machine's unique MachineGuid identifier. This progression reflects heightened operational sophistication focused on defeating signature-based perimeter defenses and deep packet inspection firewalls.

STRATEGIC RISK PERSPECTIVE: The weaponization of standard messaging architectures (MQTT and Matrix) allows adversarial traffic to blend invisibly with legitimate business communications. This tactical evolution significantly degrades the effectiveness of traditional perimeter detection, demanding enhanced host behavioral monitoring and rigorous protocol-level controls.

2. TECHNICAL ARCHITECTURE & EXECUTION LIFECYCLE

Initial intrusion vectors and lateral propagation rely on compromised credentials executed via Windows Remote Management (WinRM), facilitated by penetration testing frameworks including EVIL-WINRM and WINRM-FS. The payloads execute as interactive binaries or establish

persistent system access by installing dedicated Windows background services via the `--install` argument. The registered services are titled `cp\support` and `wtas`, respectively. Upon initialization, each implant searches for a configuration file (`config.toml`) in local directories or default storage paths such as `%PROGRAMDATA%\cp\support\config.toml` and `%PROGRAMDATA%\SynapseAgent\config.toml`. If an unencrypted configuration is parsed, the backdoor encrypts sensitive configuration parameters using ChaCha20-Poly1305. The encryption key is derived directly from `HKLM\Software\Microsoft\Cryptography\MachineGuid`, ensuring the implant executes strictly on the compromised endpoint. Forensic extraction and sandbox execution on external systems trigger decryption failures, causing immediate process termination.

BACKDOOR VARIANT	PERSISTENCE MECHANISM	C2 INFRASTRUCTURE / PROTOCOL	EXECUTION SUBSYSTEM
MQTT-BIRD-AGENT (Version 0.1.0)	Windows Service: <code>cp\support</code> . Retains encrypted <code>config.toml</code> file on disk.	HiveMQ MQTT Broker (<code>broker.hivemq.com:8883</code>). Endpoints: <code>/status</code> , <code>/metrics</code> , <code>/cmd/ req</code>	<code>PowerShell.exe</code> executed in hidden mode (<code>-NonInteractive -NoProfile -Command</code>)
MATRIX-BIRD-AGENT (Version 0.1.0)	Windows Service: <code>wtas</code> . Deletes disk file; persists sealed config in Registry.	Actor Element server (<code>meet.element[.]tw</code>). Matrix Events: <code>m.bird.status</code> , <code>m.bird.metrics</code>	Standard Windows Command Shell (<code>cmd.exe</code>); commands dispatched by user <code>panel-bot</code>

The persistence mechanisms of both variants reveal deliberate operational divergence. The HiveMQ variant preserves its partially encrypted configuration file on disk. In contrast, the Element variant deletes the on-disk `config.toml` immediately following initialization and stores the sealed configuration parameters exclusively within the registry path `HKLM\Software\synapse\Config\SealedConfig`, significantly reducing its on-disk footprint.

Outbound communication begins with an HTTP GET request to `http://ip-api.com/json` to log external IP addresses and geolocation. System telemetry (CPU utilization and memory load) is exfiltrated periodically. Commands received across both variants return structured responses containing process `stdout`, `stderr`, exit code, and execution duration.

3. TECHNICAL CONFIGURATION SPECIFICATIONS

Reverse engineering of decrypted configuration artifacts highlights structured operational parameters controlling command routing, reporting intervals, and cryptographic authentication:

[Artifact Specification: HiveMQ Variant (config.toml)] [agent]

```
id = "hostname.domain"
metrics_interval = 30
```

```
[mqtt] host =
"broker.hivemq.com" port =
8883
```

```
[seal] blob =
"484bca1dce4f94b263cab99bb13f03430c2905692906561304b5060056cbce25..."
```

```
Decrypted Blob Parameters: channel_id : a65eab97e41a92d23e11dcfa agent_privkey
: afa1770f37f32e6f4c8ce8c02ca6f6db486056838033f3588723ac6b server_pubkey :
a93b9bb77f69cafe3faacc7c8607e3e4cc01e64a8393ec9da7ac4641bcab5e5f
```

[Artifact Specification: Element / Matrix Variant (Registry Staged)] {

```
"agent": {
  "id": "hostname-domain",
  "metrics_interval": 30
},
"matrix": {
  "homeserver": "https://meet.element.tw",
  "username": "synapse-hostname",
  "room_id": "!HcJjf78Ste3TSMW72EpeHPms8_6DcJz7YEsixgLUbm4",
  "access_token": ""
},
"seal": {
  "blob": "X7wNnN1cylt9FJcAxXA4BgX4aj6GmBoL"
}
}
```

4. THREAT ACTOR EVOLUTION & CONCLUSION

The operational evolution of Toy Ghouls illustrates a clear trajectory toward engineering sophistication. Having transitioned from public tools and leaked codebases to custom ransomware (GenieLocker) and now bespoke modular backdoors, the actor prioritizes persistence and defense evasion.

Routing C2 communications through legitimate MQTT brokers and self-hosted Element messaging nodes complicates threat-hunting efforts. Given this trajectory of custom malware engineering, security teams must anticipate expanded targeting, enhanced anti-analysis techniques, and further refinement of evasion mechanisms in future campaigns.

5. STRATEGIC & OPERATIONAL DEFENSE RECOMMENDATIONS

Organizations should implement the following strategic and technical mitigations to safeguard against Angry Birds backdoor activity:

- 1. HARDEN REMOTE MANAGEMENT PROTOCOLS:** Restrict Windows Remote Management (WinRM) accessibility strictly to authorized management subnets and jump hosts. Enforce multi-factor authentication (MFA) and enforce complex, rotated service credentials.
- 2. RESTRICT EGRESS NETWORK PROTOCOLS:** Enforce strict egress firewall filtering. Block or monitor outbound connections over port 8883 (MQTT TLS) and restrict outbound traffic to unapproved Matrix/Element domains, specifically `meet.element[.]tw`.

- DEPLOY BEHAVIORAL ENDPOINT DETECTION & RESPONSE (EDR):** Establish behavioral telemetry to flag unauthorized Windows service creation (specifically `cp\support` and `wtas`) and monitor modifications within `HKLM\Software\synapse\` and `HKLM\Software\SynapseAgent\`.
- CENTRALIZE SCRIPT BLOCK & PROCESS AUDITING:** Enable PowerShell Script Block Logging (Event ID 4104) and transcription logging. Monitor command execution patterns involving hidden PowerShell parameters (`-NonInteractive` `-NoProfile`).
- SUPERVISE FILESYSTEM ARTIFACTS:** Audit directory activity within `%PROGRAMDATA%` for unexpected `.toml` file drops or rapid configuration file deletions.
- INGEST THREAT INTELLIGENCE & IOCS:** Ingest verified Indicators of Compromise into enterprise SIEM and Next-Generation Firewalls for continuous automated blocking and threat detection.

6. INDICATORS OF COMPROMISE (IOCS)

INDICATOR / OBSERVABLE	INDICATOR TYPE	OPERATIONAL DESCRIPTION
<code>meet.element[.]tw</code>	Domain / Hostname	Malicious Element/Matrix Command-and-Control Server
<code>7916C33688385525078BEE504C90F359</code>	MD5 File Hash	Angry Birds Backdoor Executable (mqtt-bird-agent)
<code>BFADBEEE63A4F0BF19EC9DEB8FA58F58</code>	MD5 File Hash	Angry Birds Backdoor Executable (matrix-bird-agent)
<code>broker.hivemq.com:8883</code>	Network Socket	Public MQTT Broker Infrastructure Relay Channel C2
<code>http://ip-api[.]com/json</code>	URL / Service	Victim Public IP Reconnaissance Lookup Endpoint

7. REFERENCES & PRACTICE INFORMATION

PRIMARY RESEARCH REFERENCE: Drona Research and Intelligence Labs (DRIL) Technical Advisory; Kaspersky Securelist Threat Intelligence Research: **TOY GHOULS: NEW HIVEMQ AND ELEMENT BACKDOORS** (Referenced via <https://securelist.com/toy-ghouls-new-hivemq-and-element-backdoors/121270/>).

PRACTICE DISCLAIMER: This document is delivered under Traffic Light Protocol (TLP) GREEN standards for enterprise risk remediation and strategic resilience planning. Recipients may share this intelligence internally across organizational IT/OT defense units. No warranty, expressed or implied, is provided regarding adversarial tactics evolving beyond the observation timeframe.



**Securing Today,
Empowering Tomorrow**



Drona Cyber Sloutions



info@dronacybersolutions.com



+91 81609 68270



www.dronacybersolutions.com