Pivot Infrastructure Analysis: Frankenstein Variant of ToneShell Backdoor Targeting Myanmar

Author: Pisut Muangsamai
Date: 15 Sep 2025
Classification: TLP:CLEAR

1. Executive Summary

This report presents the results of pivot-based infrastructure analysis centered on a Command-and-Control (C2) server **146[.]70[.]29[.]229** associated with the **Frankenstein variant of the ToneShell backdoor**, a malware tied to the **China-nexus Mustang Panda APT group**.

The variant was reported by Intezer in attacks against **Myanmar**, a region of strategic interest to China. Although the variant itself does not include significant new capabilities, it uses advanced anti-analysis techniques and new infrastructure.

Using this confirmed C2 as a **pivot point**, we enumerated and correlated additional IP infrastructure that share overlapping attributes and may be **currently or in the future leveraged as C2 servers by the same threat actor**.

2. Background: Mustang Panda & ToneShell

- **Mustang Panda (a.k.a. TA416)** is a long-running China-linked threat actor known for cyberespionage targeting Southeast Asia, EU entities, and NGOs.
- **ToneShell** is a lightweight backdoor often deployed through **DLL sideloading** and **compressed lure archives** containing **legitimately signed executables**.
- Campaigns frequently leverage **cloud storage delivery** (OneDrive, Dropbox) and **custom packers** to evade detection.
- The **Frankenstein variant** integrates known ToneShell components with **new anti-analysis logic** to hinder sandbox execution and researcher analysis.

Strategic Context: Targeting Myanmar aligns with China's geopolitical priorities involving border security, Belt & Road infrastructure projects, and political influence operations.

3. Initial Pivot: C2 146.70.29.229

3.1 Registration and ASN Details

- **IP:** 146.70.29.229
- **Subnet:** 146.70.16.0/20
- **ASN:** AS9009 (M247 Europe SRL)
- **WHOIS Org:** M247 Ltd, Singapore Infrastructure

3.2 Exposed Services

Port	Protocol	Service	Notes
TCP 26263	RDP	Remote Desktop	Non-standard RDP port
TCP 5985	WinRM	Windows Remote Management	HTTP API enabled

- **TLS Cert Fingerprint:** 1e1066f0cf558dc988745be4068afb5e034178f9cc55d64bb6c2451b9beedbcf
- **Subject / Issuer CN:** WIN-25FFVSIPLS1
- **Observed Hostname:** WIN-25FFVSIPLS1
- **Last Seen:** 15 Sep 2025 (Censys)

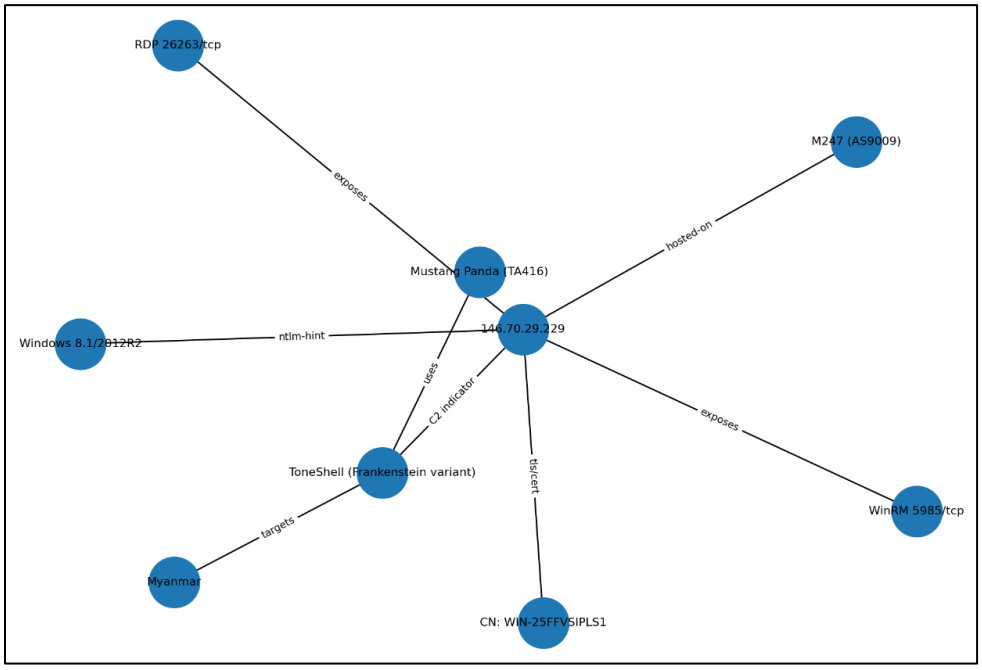
4. Infrastructure Pivoting Methodology

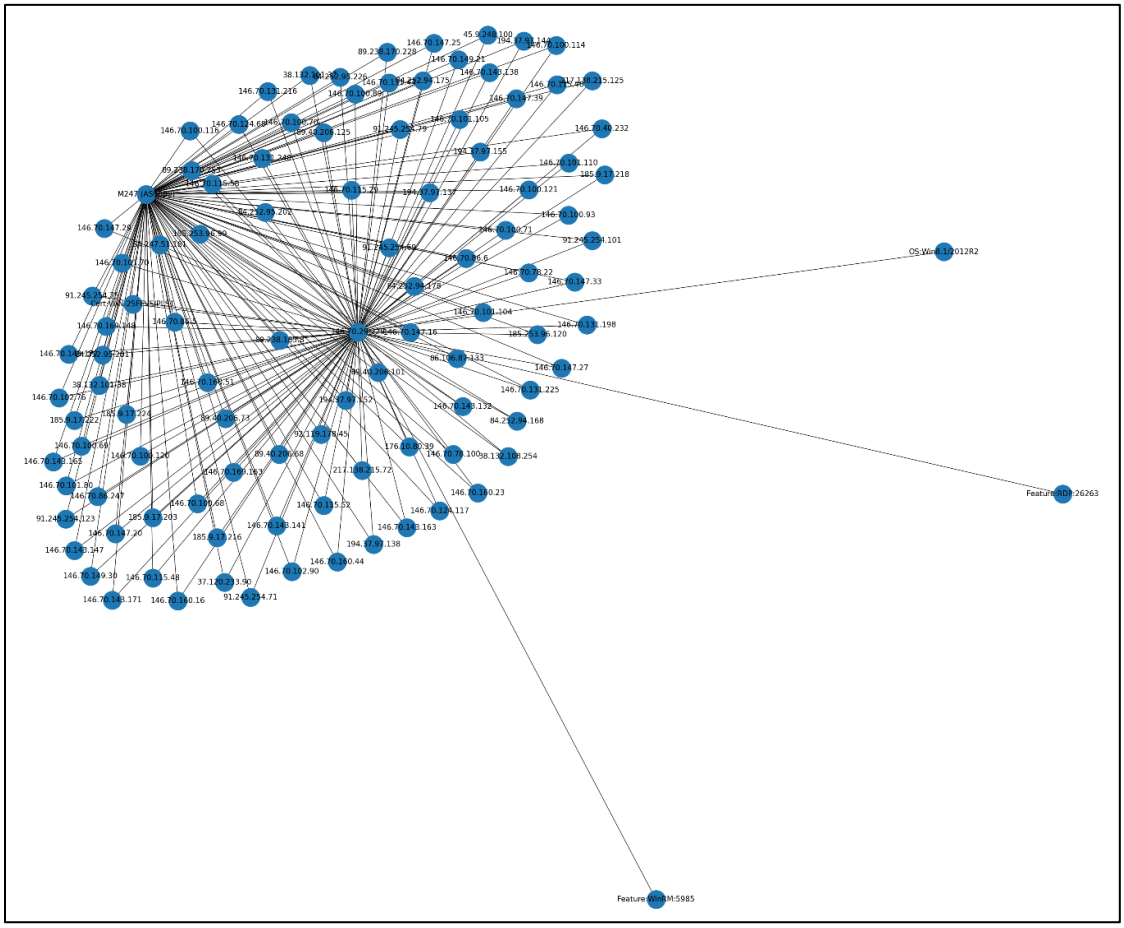
To identify related infrastructure, we pivoted from the known C2 across multiple data sources (Censys, Fofa, WHOIS, Shodan):

Correlation Criteria:

- Hosting provider: **M247 Ltd / AS9009**
- Similar rare exposed services: **RDP on non-standard high ports (e.g., 26263)**, **WinRM (5985)**
- Matching TLS certificate attributes (CN = WIN-25FFVSIPLS1)
- Similar OS fingerprinting: **Windows 8.1 / Server 2012 R2 (NTLM info)**
- Temporal co-observation (similar last-seen timestamps)
- Overlapping network blocks (e.g. 146.70.16.0/20, 146.70.100.0/24, 185.9.17.0/24)

This produced a cluster of **100 high-confidence related IPs** potentially usable as future C2 infrastructure.





5. Identified Suspected Infrastructure (High Risk)

Full list of 100 IPs is maintained in the Appendix. These IPs are spread across numerous M247-assigned netblocks including **146.70.40.0/24, 146.70.100.0/24, 146.70.131.0/24, 185.9.17.0/24, 194.37.97.0/24**.

6. Threat Intelligence Assessment

- **Attribution Confidence:** Medium - Based on infrastructure clustering and behavioral fingerprints.
- **Future Use Likelihood:** High - Threat actors often maintain pools of ready servers for rotation / fallback.
- **Risk to Organizations:** High - Potential hosting of C2 nodes, malware staging servers, or phishing infra.

Analyst Note: Mustang Panda frequently reuses bulletproof hosting providers (like M247) and rotates among pre-staged systems. This cluster may serve as a staging pool for future campaigns in Southeast Asia, especially Myanmar, Laos, and Thailand.

7. Recommendations

For SOC and detection teams, add the identified IP addresses to your threat-hunting blocklists and SIEM enrichment rules, continuously monitor for outbound TCP traffic that exhibits TLS-like record headers on port 443 as well as any connections from end-user devices to AS9009 infrastructure, and enrich DNS and NetFlow telemetry to correlate and investigate any contact attempts.

For CTI teams, tag these IP addresses as "**Suspected Mustang Panda Infrastructure**" within MISP or OpenCTI, track subsequent DNS resolutions, certificate changes, and service/port activity over time, and share the indicators through established threat-intelligence channels such as ThaiCERT and relevant MISP communities.

For policy and governance stakeholders, include M247 (AS9009) ranges in geopolitical, risk-based access reviews, and implement geo-blocking or at minimum heightened monitoring for traffic destined to servers in Myanmar or adjacent high-risk regions.

8. Appendix - Full List of Related IPs

37[.]120[.]233[.]90

38[.]132[.]101[.]37

38[.]132[.]101[.]38

38[.]132[.]108[.]254

45[.]9[.]248[.]100

84[.]247[.]51[.]181

84[.]252[.]94[.]168

84[.]252[.]94[.]175

84[.]252[.]94[.]178

84[.]252[.]95[.]201

84[.]252[.]95[.]202

84[.]252[.]95[.]226

86[.]106[.]87[.]133

89[.]40[.]206[.]68

89[.]40[.]206[.]73

89[.]40[.]206[.]101

89[.]40[.]206[.]125

89[.]238[.]170[.]228

89[.]238[.]170[.]253

89[.]238[.]185[.]8

91[.]245[.]254[.]69

91[.]245[.]254[.]71

91[.]245[.]254[.]75

91[.]245[.]254[.]79

91[.]245[.]254[.]101

91[.]245[.]254[.]123

92[.]119[.]178[.]45

146[.]70[.]40[.]232

146[.]70[.]78[.]22

146[.]70[.]78[.]100

146[.]70[.]86[.]5

146[.]70[.]86[.]6

146[.]70[.]86[.]247

146[.]70[.]100[.]68

146[.]70[.]100[.]69

146[.]70[.]100[.]70

146[.]70[.]100[.]71

146[.]70[.]100[.]89

146[.]70[.]100[.]93

146[.]70[.]100[.]114

146[.]70[.]100[.]116

146[.]70[.]100[.]120

146[.]70[.]100[.]121

146[.]70[.]101[.]70

146[.]70[.]101[.]80

146[.]70[.]101[.]104

146[.]70[.]101[.]105

146[.]70[.]101[.]110

146[.]70[.]102[.]76

146[.]70[.]102[.]90

146[.]70[.]115[.]29

146[.]70[.]115[.]46

146[.]70[.]115[.]48

146[.]70[.]115[.]52

146[.]70[.]115[.]58

146[.]70[.]124[.]68

146[.]70[.]124[.]117

146[.]70[.]131[.]44

146[.]70[.]131[.]198

146[.]70[.]131[.]216

146[.]70[.]131[.]225

146[.]70[.]131[.]248

146[.]70[.]143[.]132

146[.]70[.]143[.]138

146[.]70[.]143[.]141

146[.]70[.]143[.]147

146[.]70[.]143[.]163

146[.]70[.]143[.]165

146[.]70[.]143[.]171

146[.]70[.]143[.]172

146[.]70[.]147[.]16

146[.]70[.]147[.]20

146[.]70[.]147[.]25

146[.]70[.]147[.]27

146[.]70[.]147[.]29

146[.]70[.]147[.]33

146[.]70[.]147[.]39

146[.]70[.]149[.]21

146[.]70[.]149[.]30

146[.]70[.]160[.]16

146[.]70[.]160[.]23

146[.]70[.]160[.]44

146[.]70[.]160[.]51

146[.]70[.]169[.]148

146[.]70[.]169[.]163

176[.]10[.]80[.]39

185[.]9[.]17[.]203

185[.]9[.]17[.]216

185[.]9[.]17[.]218

185[.]9[.]17[.]222

185[.]9[.]17[.]224

185[.]253[.]96[.]99

185[.]253[.]96[.]120

194[.]37[.]97[.]137

194[.]37[.]97[.]138

194[.]37[.]97[.]144

194[.]37[.]97[.]152

194[.]37[.]97[.]155

217[.]138[.]215[.]72

217[.]138[.]215[.]125

9. References

- Fishbein, N. (2025, September 10). *Frankenstein variant of the ToneShell backdoor targeting Myanmar*. Intezer. https://intezer.com/blog/frankenstein-variant-of-the-toneshell-backdoor-targeting-myanmar/
- Censys. (2025, September 13 -15). *Search results for IP 146.70.29.229 and related infrastructure* [Data set]. Retrieved September 15, 2025, from https://search.censys.io/
- FOFA. (2025, September 13 -15). *Search results for IP 146.70.29.229 and related infrastructure* [Data set]. Retrieved September 15, 2025, from https://fofa.info/

- RIPE NCC. (2025, September 13 -15). *WHOIS record for 146.70.29.229 and AS9009* [Data set]. Retrieved September 15, 2025, from https://www.ripe.net/