V1.0 / July. 2025

From a single IP/Domain to a C2 infrastructure:

Proactive Threat Hunting with Malware C2

Charles

TEAMT5
杜 浦 數 位 安 全
Persistent Cyber Threat Hunters

AGENDA

TEAMT5
杜 浦 數 位 安 全

01 CTI based Active Cyber Defense

02 What is C2 Pivoting

03 How to do C2 Pivoting

04 Case Study

05 Conclusion

CTI based Active Cyber Defense

Japan's Active Cyber Defense Law

TEAMT5 杜浦數位安全

- Active Cyber Defense: Proactive measures taken to detect, analyze, and respond to cyber threats in real time.
- The purpose: Enable Japan to "identify and respond to cyber attacks more quickly and effectively"

Cyber Threat Intelligence (CTI)

TEAMT5 杜浦數位安全

- CTI: Collection, analysis, and dissemination of information about current and potential cyber threats.

- The core concept of CTI:
  - "**Know your enemy** and know yourself and you can fight a hundred battles without disaster." – Sun Tzu

How CTI supports ACD

TEAMT5
杜 浦 數 位 安 全

Cyber Threat Intelligence	→	Active Cyber Defense
Provides early warning of threats	→	Enables rapid detection and blocking of known threats
Supplies IOCs and TTPs	→	Feeds detection rules, SIEM alerts, and automated response tools
Informs risk-based prioritization	→	Helps defenders focus resources on high-impact threats
Tracks adversary behavior over time	→	Improves response effectiveness and predictive defense
Contextualizes alerts (who, why, what)	→	Reduces false positives and improves response accuracy

What is C2 Pivoting

C2 infrastructure

TEAMT5
杜 浦 數 位 安 全

- **Command and Control (C2) infrastructure** refers to the networked systems, servers, domains, and communication channels used by threat actors to **remotely control compromised devices**, **exfiltrate data**, or **issue commands** to malware during an attack.

- In CTI analysis, understanding C2 infrastructure helps analysts:
  - Attribute attacks to known threat actors
  - Discover related campaigns (via infrastructure reuse)
  - Block or sinkhole malicious traffic
  - Map the operational footprint of adversaries

C2 Pivoting

TEAMT5
杜 浦 數 位 安 全

- **C2 Pivoting**: In CTI, A process using known **Command and Control (C2) infrastructure indicators** (e.g., IPs, domains, SSL certs) to **discover additional related threat activity**, infrastructure, or campaigns in cyber threat intelligence.

C2 Pivoting

TEAMT5
杜 浦 數 位 安 全

- Purpose:
  - Expand knowledge of attacker infrastructure
  - Link threats to known APT groups
  - Enhance threat detection and hunting
  - Support attribution and proactive defense

How to do C2 Pivoting

How to do C2 Pivoting

TEAMT5 杜浦數位安全

- Malware Analysis
- Incident Response

- C2 IP
- Domain

Map attacker's C2 infrastructure

Query
- ✓ PDNS
- ✓ WHOIS
- ✓ SSL Certificate

Verify with
- Registrar
- ASN
- DN Pattern
- Open Port
- Malware

Traps / Obstacles in C2 Pivoting

TEAMT5
杜 浦 數 位 安 全

- False Attribution from Shared Infrastructure (Shared web hosting)
- Parking IP addresses
- Outdated Indicators (Sinkhole)
- Overreliance on Automation
- Over-Pivoting (Intel. Pollution)
- Advanced techniques to hide C2 (e.g. domain fronting)

Case Study

Case 1

TEAMT5
杜 浦 數 位 安 全

- You discovered a SoftEther VPN C2 IP, 122.10.89.230

Case 2

TEAMT5
杜 浦 數 位 安 全

- A C2 IP, 38.54.63.20, used by Social Network Team in Aug. 2023

Conclusion

Conclusion

- Threat actors tend to build different layers of C2 infrastructure with different tool sets. They will be used interchangeably in a campaign, to prevent from blocked by firewalls
- C2 Pivoting could help active cyber defense:
  - Achieving better defense by knowing more C2, TTPs
  - Obtaining a broader view of an observed operation
  - Understanding who is your adversary
- C2 Pivoting could be challenging sometimes since actors are also evolving
- Happy hunting your adversaries!

THANK YOU!

Charles

charles@teamt5.org

TEAMT5

杜 浦 數 位 安 全

Persistent Cyber Threat Hunters