
GENERAL:

First Seen Time and Date: 25/08/2022 20:09:16 +0500
Insight: Recon Using Common Windows Commands with Threat Intel Matches

Associated Signals:

1. Recon Using Common Windows Commands
2. Threat Intel - Device IP Matched Threat Intel File Hash
3. Threat Intel - Device IP Matched Threat Intel File Hash
4. Threat Intel - Device IP Matched Threat Intel File Hash
5. Threat Intel - Device IP Matched Threat Intel File Hash
6. Threat Intel - Device IP Matched Threat Intel File Hash
7. Threat Intel - Device IP Matched Threat Intel File Hash
8. IPCONFIG Command Executed

SEVERITY CLASSIFICATION:

Priority: P1

Reason: This incident is classified as **P1 Critical** due to confirmed evidence of malicious reconnaissance activity (systeminfo, ipconfig) on a domain controller (**dc.windomain.local**) combined with multiple threat intelligence matches to known **APT file hashes**. The overlap of suspicious user activity (local discovery commands) and threat intel indicators (APT-related malware artifacts) suggests active compromise of a critical infrastructure host (domain controller).

SOURCE DETAILS:

Source Device: dc.windomain.local
Source Device IP: 192.168.38.102
User: vagrant

Observed Commands:

- systeminfo (System discovery)
- ipconfig (Network configuration discovery)

MITRE ATT&CK Mapping:

- **TA0007 – Discovery**
    - **T1018 – Remote System Discovery**
    - **T1082 – System Information Discovery**
    - **T1016 – System Network Configuration Discovery**

TARGET DETAILS:

Target Host: Domain Controller – dc.windomain.local
Target Username: vagrant
Target IP: 192.168.38.102
Criticality: High (DC is a core infrastructure component)

ADDITIONAL INFORMATION:

- **File Hash Detection:**
    - YQICQ6N4_SETUP.zip flagged via CrowdStrike Falcon detection.
    - Matches multiple intel sources: threat_FileHash_APT_IOCs, threat_FileHash_APTs.
    - Indicates known APT-related malicious file hash.
- **Field Tags:** default_accounts, PCI → suggests potential compliance impact if data exfiltration occurred.

INCIDENT DETAILS:

Between **25/08/2022 20:09 and 26/08/2022 08:15**, the following sequence of suspicious activity was observed on **dc.windomain.local**:

1. At **20:09**, user vagrant executed reconnaissance commands:
    - systeminfo.exe → system discovery.
    - ipconfig.exe → network discovery.
2. Shortly after, CrowdStrike detected the presence of suspicious archive YQICQ6N4_SETUP.zip, which matched multiple known **APT file hashes**.

3. The IOC match indicates possible **malware installation or staging** by a known APT group on the domain controller.
4. Recon activity combined with APT-related file indicators strongly suggests **early-stage compromise with potential lateral movement preparation**.

REMEDIATION ACTIONS:

Immediate Containment:

- Isolate the domain controller dc.windomain.local (192.168.38.102) from the network.
- Disable user account vagrant until investigation is complete.
- Block identified malicious file hash across EDR/AV solutions.

Forensic Investigation:

- Collect memory, process, and file system artifacts from the DC for malware analysis.
- Validate whether YQICQ6N4_SETUP.zip was executed and whether persistence mechanisms were created.
- Search across environment for additional **instances of the malicious hash**.
- Investigate how user vagrant executed commands (compromised credentials vs insider).

Environment Hardening:

- Review domain controller logs for **lateral movement attempts**.
- Reset credentials for high-privilege accounts.
- Deploy **honeytokens/canary accounts** to detect further reconnaissance.
- Increase monitoring of critical system commands (systeminfo, net, ipconfig, etc.) in domain controllers.

Conclusion:

This is a **P1 Critical** incident. The combination of **local recon commands** on a **domain controller** with **APT-linked file hash matches** strongly suggests compromise by a **sophisticated threat actor**. Containment and forensic analysis are required immediately to prevent further spread and potential domain-wide impact.
